Manual del usuario



Switches administrados Ethernet Stratix 5700









Allen-Bradley • Rockwell Software

Rockwell Automation

Información importante para el usuario

Lea este documento y los documentos enumerados en la sección Recursos adicionales sobre la instalación, configuración y operación de este equipo antes de instalar, configurar, operar o realizar el mantenimiento de este producto. Los usuarios deben familiarizarse con las instrucciones de instalación y cableado, y con los requisitos de todos los códigos, leyes y estándares aplicables.

Las actividades que incluyan instalación, ajustes, puesta en servicio, uso, montaje, desmontaje y mantenimiento deberán ser realizadas por personal debidamente capacitado de conformidad con el código de prácticas aplicable.

Si este equipo se utiliza de una forma diferente a la indicada por el fabricante, la protección proporcionada por el equipo puede verse afectada.

En ningún caso Rockwell Automation, Inc. responderá ni será responsable de los daños indirectos o consecuentes que resulten del uso o la aplicación de este equipo.

Los ejemplos y los diagramas que aparecen en este manual se incluyen únicamente con fines ilustrativos. Debido a las numerosas variables y requisitos asociados con cada instalación en particular, Rockwell Automation, Inc. no puede asumir ninguna responsabilidad ni obligación por el uso basado en los ejemplos y los diagramas.

Rockwell Automation, Inc. no asume ninguna responsabilidad de patente con respecto al uso de la información, los circuitos, los equipos o el software descritos en este manual.

Este manual contiene notas de seguridad en cada circunstancia en que se estimen necesarias.

	**ADVERTENCIA:** Identifica información acerca de prácticas o circunstancias que pueden causar una explosión en un ambiente peligroso que, a su vez, puede ocasionar lesiones personales o la muerte, daños materiales o pérdidas económicas.
	**ATENCIÓN:** Identifica información acerca de prácticas o circunstancias que pueden ocasionar lesiones personales o a la muerte, daños materiales o pérdidas económicas. Estas notas de atención le ayudan a identificar un peligro, evitarlo y reconocer las posibles consecuencias.
IMPORTANTE	Identifica información esencial para la correcta aplicación y comprensión del funcionamiento del producto.

También puede haber etiquetas sobre el equipo o dentro del mismo, con el fin de recomendar precauciones específicas.

	**PELIGRO DE CHOQUE:** Puede haber etiquetas en el exterior o en el interior del equipo (por ejemplo, en un variador o un motor) para advertir sobre la posible presencia de voltajes peligrosos.
	**PELIGRO DE QUEMADURA:** Puede haber etiquetas en el exterior o en el interior del equipo (por ejemplo, en un variador o un motor) a fin de advertir sobre superficies que podrían alcanzar temperaturas peligrosas.
	**RIESGO DE ARCO ELÉCTRICO:** Puede haber etiquetas sobre el equipo o dentro del mismo (por ejemplo, en un centro de control de motores) para alertar sobre la posibilidad de que se produzca un arco eléctrico. Un arco eléctrico ocasionará lesiones graves o la muerte. Use un equipo de protección personal (PPE) adecuado. Siga TODOS los requisitos reglamentarios en torno a las prácticas de trabajo seguras y al equipo de protección personal (PPE).

Resumen de cambios

Este manual contiene información nueva y actualizada.

Información nueva y actualizada

Esta tabla contiene los cambios realizados en esta revisión.

Tema	Página
Requisitos actualizados de hardware y software del administrador de dispositivos	24, 50
Nueva ventana Express Setup	52, 52
Nuevo proceso para habilitar el encaminamiento	91
Nueva interface web del administrador de dispositivos	95…162

Notas:

Prefacio

Capítulo 1

Acerca de los switches

Capítulo 2

Instalación del switch

Capítulo 3

Características del software del switch

Capítulo 4

Administración del switch mediante la interface web del administrador de dispositivos

Capítulo 5

Administración del switch mediante el ambiente Studio 5000

Capítulo 6

Resolución de problemas del switch

Apéndice A

Tipos de datos definidos por módulos

Apéndice B

Asignaciones de puertos para datos CIP

Apéndice C

Cables y conectores

Apéndice D

Historial de cambios

Índice

Esta publicación describe las características del software incorporado y las herramientas para configurar y administrar los switches administrados Ethernet Stratix 5700™. Además, esta publicación incluye información sobre la resolución de problemas que le ayudará a resolver problemas básicos del switch y de la red.

Utilice este manual cuando necesite configurar y monitorear switches administrados Ethernet Stratix 5700. Este manual supone que está familiarizado con lo siguiente:

- Conceptos fundamentales de switches de redes de área local (LAN)
- Conceptos y terminología del protocolo Ethernet y de redes de área local

Ambiente Studio 5000

El ambiente de ingeniería y diseño Studio 5000™ combina elementos de ingeniería y diseño en un ambiente común. El primer elemento en el ambiente Studio 5000 es la aplicación Logix Designer. Logix Designer es el nuevo nombre de marca asignado a la aplicación de software RSLogix™ 5000, y continuará siendo el producto para programar los controladores Logix5000™ en soluciones discretas, de procesos, de lotes, de control de movimiento, de seguridad y basadas en variadores.

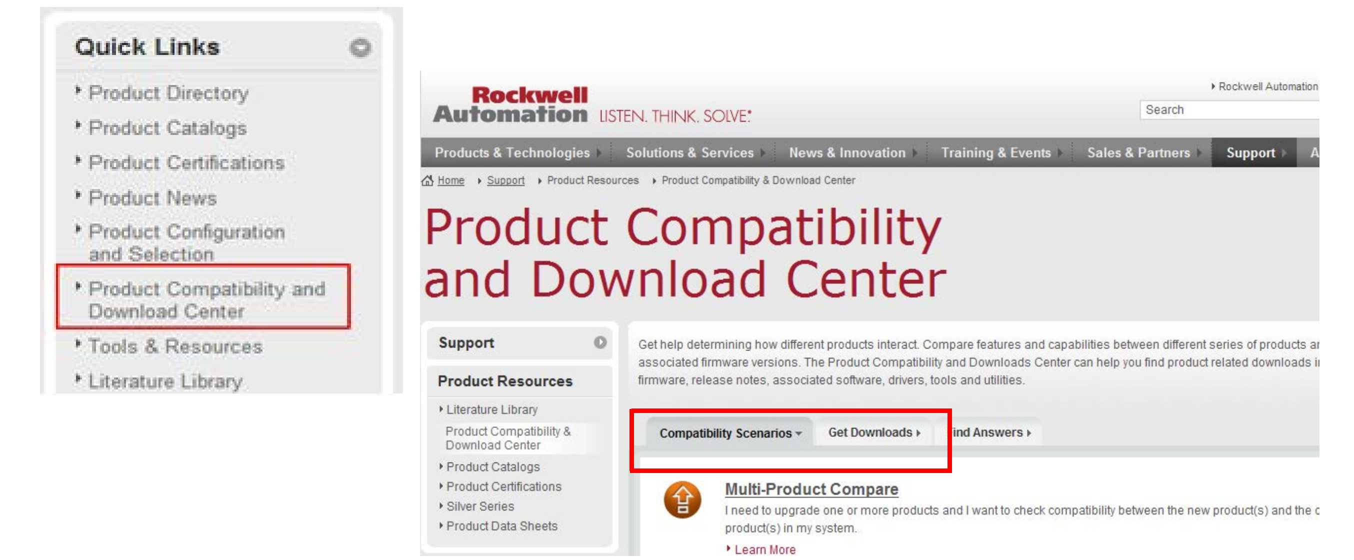


El ambiente Studio 5000 constituye la base para las futuras herramientas y capacidades de diseño de ingeniería de Rockwell Automation®. Este ambiente es el lugar donde los ingenieros de diseño desarrollan todos los elementos de sus sistemas de control.

Acceso a las notas de la versión del producto

Las notas de la versión del producto se encuentran disponibles en línea en el Product Compatibility and Download Center.

1. En la lista Quick Links en http://www.ab.com, haga clic en Product Compatibility and Download Center.



2. En las fichas Compatibility Scenarios o Get Downloads, busque y elija su producto.



3. Haga clic en el icono de descarga para obtener acceso a las notas de la versión del producto.

Recursos adicionales

Estos documentos contienen información adicional relativa a productos relacionados de Rockwell Automation.

Recurso	Descripción
Stratix Ethernet Managed Switches Technical Data, publicación 1783-TD001	Proporciona las especificaciones de los switches.
Ethernet Design Considerations Reference Manual, publicación ENET-RM002	Proporciona información sobre la implementación de un sistema basado en la plataforma EtherNet/IP.
Ayuda en línea de la interface web del administrador de dispositivos (proporcionada con el switch)	Proporciona información sensible al contexto sobre la configuración y el uso del switch, incluidos los mensajes del sistema.
Pautas de cableado y conexión a tierra de equipos de automatización industrial, publicación 1770-4.1	Proporciona pautas generales para la instalación de un sistema industrial de Rockwell Automation.
Sitio web de certificaciones de productos, http://www.ab.com	Proporciona declaraciones de cumplimiento normativo, certificados y otros detalles sobre las certificaciones.

Puede ver o descargar las publicaciones desde http:/www.rockwellautomation.com/literature/. Para solicitar copias impresas de la documentación técnica, comuníquese con el distribuidor de Allen-Bradley o representante de ventas de Rockwell Automation correspondientes a su localidad.

Para obtener información sobre otras características del software o la configuración, consulte las siguientes publicaciones de Cisco en http://www.Cisco.com:

- Cisco IE-2000 Command Line Reference Manual
- Cisco IE-2000 Software Configuration Guide
- Cisco IE-2000 Switch System Message Guide

Notas:

Acerca de los switches

Los switches administrados Ethernet Stratix 5700 proporcionan una infraestructura de conmutación segura para ambientes hostiles. Puede conectar estos switches a dispositivos de red como servidores, encaminadores y otros switches. En ambientes industriales puede conectar dispositivos de comunicación industrial habilitados para Ethernet como, por ejemplo, controladores lógicos programables (PLC), interfaces operador-máquina (HMI), variadores, sensores y E/S.

Números de catálogo de los switches

Estos switches Stratix 5700 se encuentran disponibles en dos versiones de firmware: la versión Lite y la versión completa.

Número de catálogo	Descripción
1783-BMS06SL	Switch administrado de 6 puertos (4 puertos Ethernet; 2 ranuras SFP); firmware Lite
1783-BMS06SA	Switch administrado de 6 puertos (4 puertos Ethernet; 2 ranuras SFP); firmware completo
1783-BMS06TL	Switch administrado de 6 puertos (6 puertos Ethernet); firmware Lite
1783-BMS06TA	Switch administrado de 6 puertos (6 puertos Ethernet); firmware completo
1783-BMS06SGL	Switch administrado de 6 puertos (4 puertos Ethernet; 2 ranuras SFP Gigabit); firmware Lite
1783-BMS06SGA	Switch administrado de 6 puertos (4 puertos Ethernet; 2 ranuras SFP Gigabit); firmware completo
1783-BMS06TGL	Switch administrado de 6 puertos (4 puertos Ethernet; 2 puertos Gigabit); firmware completo
1783-BMS06TGA	Switch administrado de 6 puertos (4 puertos Ethernet; 2 puertos Gigabit); firmware completo
1783-BMS10CL	Switch administrado de 10 puertos (8 puertos Ethernet; 2 puertos combinados); firmware Lite
1783-BMS10CA	Switch administrado de 10 puertos (8 puertos Ethernet; 2 puertos combinados); firmware completo
1783-BMS10CGL	Switch administrado de 10 puertos (8 puertos Ethernet; 2 puertos Gigabit combinados); firmware Lite
1783-BMS10CGA	Switch administrado de 10 puertos (8 puertos Ethernet; 2 puertos Gigabit combinados); firmware completo
1783-BMS10CGN	Switch administrado de 10 puertos (8 puertos Ethernet; 2 puertos Gigabit combinados); firmware completo; traducción de de direcciones de red (NAT)
1783-BMS10CGP	Switch administrado de 10 puertos (8 puertos Ethernet; 2 puertos Gigabit combinados); firmware completo; protocolo de tiempo de precisión (PTP)
1783-BMS12T4E2CGNK	Switch administrado de 18 puertos (12 puertos Ethernet; 4 puertos PoE/PoE+; 2 puertos Gigabit combinados); firmware completo; NAT; revestimiento de conformación
1783-BMS12T4E2CGP	Switch administrado de 18 puertos (12 puertos Ethernet; 4 puertos PoE/PoE+; 2 puertos Gigabit combinados); firmware completo, PTP
1783-BMS12T4E2CGL	Switch administrado de 18 puertos (12 puertos Ethernet; 4 puertos PoE/PoE+; 2 puertos Gigabit combinados); firmware Lite
1783-BMS20CL	Switch administrado de 20 puertos (16 puertos Ethernet; 2 ranuras SFP; 2 puertos combinados); firmware Lite
1783-BMS20CA	Switch administrado de 20 puertos (16 puertos Ethernet; 2 ranuras SFP; 2 puertos combinados); firmware completo
1783-BMS20CGL	Switch administrado de 20 puertos (16 puertos Ethernet; 2 ranuras SFP; 2 puertos Gigabit combinados); firmware Lite
1783-BMS20CGN	Switch administrado de 20 puertos (16 puertos Ethernet; 2 ranuras SFP; 2 puertos Gigabit combinados); firmware completo; NAT
1783-BMS20CGP	Switch administrado de 20 puertos (16 puertos Ethernet; 2 ranuras SFP; 2 puertos Gigabit combinados); firmware completo; PTP
1783-BMS20CGPK	Switch administrado de 20 puertos (16 puertos Ethernet; 2 ranuras SFP; 2 puertos Gigabit combinados); firmware completo; PTP; revestimiento de conformación
Módulos SFP	
1783-SFP100FX	Transceiver de fibra multimodo 100BASE-FX
1783-SFP1GSX	Transceiver de fibra multimodo 1000BASE-SX
1783-SFP100LX	Transceiver de fibra monomodo 100BASE-LX
1783-SFP1GLX	Transceiver de fibra monomodo 1000BASE-LX
Fuente de alimentación	
Serie 1606-XL (recomendada) Serie 1606-XLP (recomendada) o equivalente	Fuentes de alimentación con salida de 24 VCC, clase 2
Tarjeta SD	
1784-SD1	Tarjeta SD industrial de 1 GB

Características del software del switch

Estas características de software se encuentran disponibles en los switches Stratix 5700.

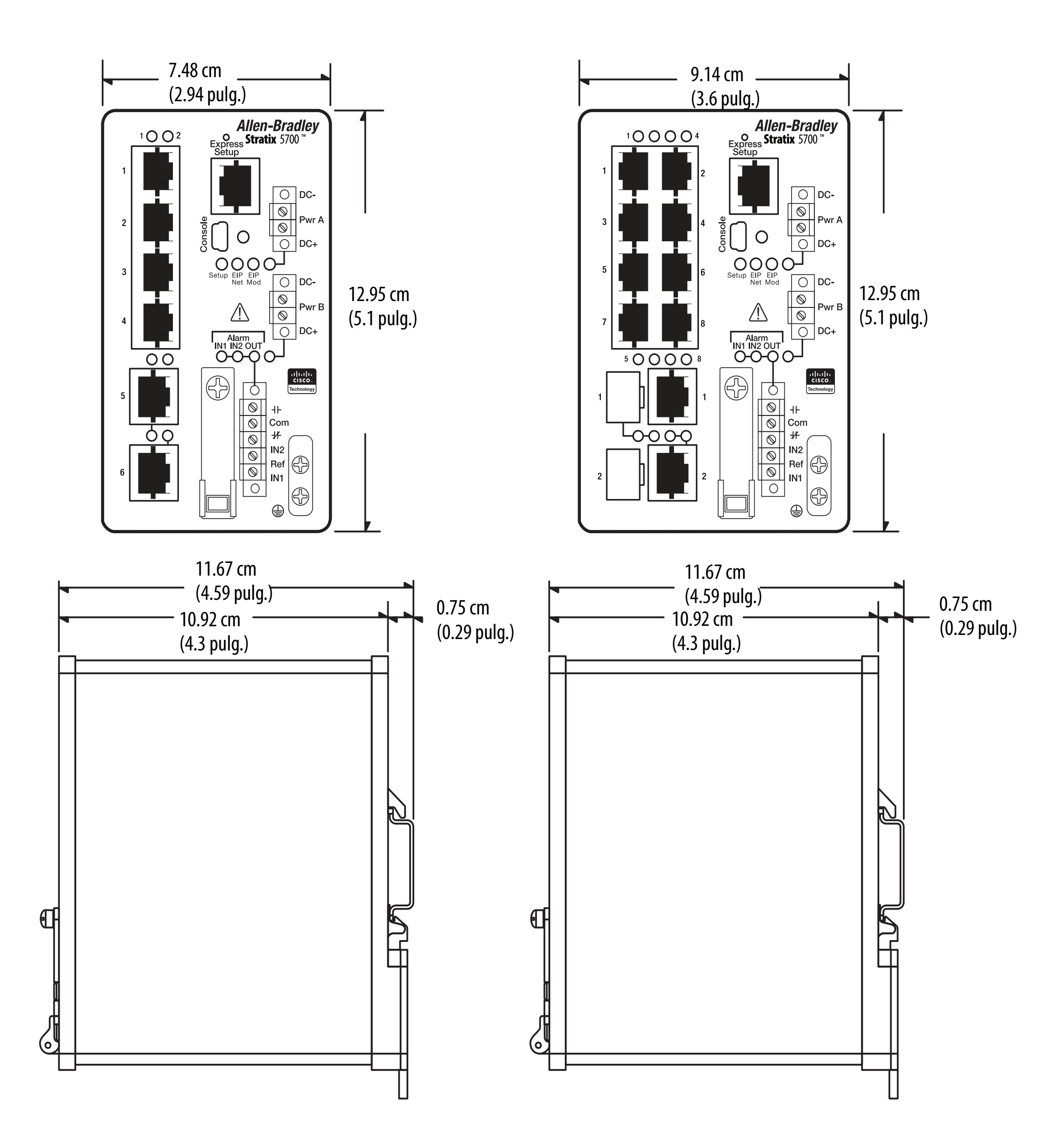
Característica	Firmware Lite	Firmware completo
CIP Sync (IEEE 1588)		Opción separada
Protocolo Ethernet resiliente (REP)	•	•
FlexLinks		•
Calidad de servicio (QoS)		•
STP, RSTP, MST (ocurrencias)	64	128
IGMP Snooping con creador de consultas	•	•
VLAN con troncalización	64	255
EtherChannel (agregación de vínculos)		•
Umbral de puerto (control de tormentas y conformación de tráfico)		•
Compatibilidad IPv6		•
Listas de control de acceso (ACL)		•
Encaminamiento estático e interVLAN		•
Control de puertos CIP y detección de fallos	•	•
Seguridad de puertos con ID MAC		•
Seguridad IEEE 802.1x		•
TACACS+, autenticación RADIUS	•	•
Cifrado (SSH, SNMPv3, HTTPS)		Firmware IOS separado disponible como ítem de catálogo separado
Puerto espejo	•	•
Syslog	•	•
Detección de cable roto	•	•
Detección de direcciones IP duplicadas		•
SNMP	•	•
Smartports	•	•
DHCP por puerto	•	•
Interface de línea de comandos (CLI)	•	•
Compatible con herramientas Cisco: Cisco Network Assistant (CNA); CiscoWorks	•	•
Interface EtherNet/IP (CIP)	•	•
Traducción de direcciones de red (NAT)		Opción separada

Dimensiones del switch

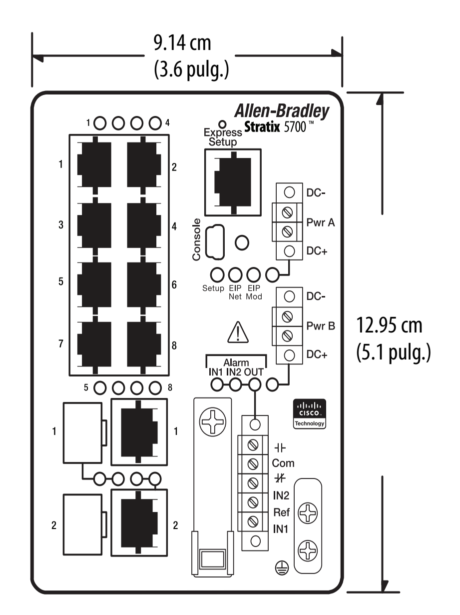
Estos diagramas representan ejemplos de los switches Stratix 5700. La conformación de cada panel frontal varía según el número de catálogo.

Switches de 6 puertos
1783-BMS06SL, 1783-BMS06SA, 1783-BMS06TL, 1783-BMS06TA, 1783-BMS06SGL, 1783-BMS06SGA, 1783-BMS06TGL, 1783-BMS06TGA

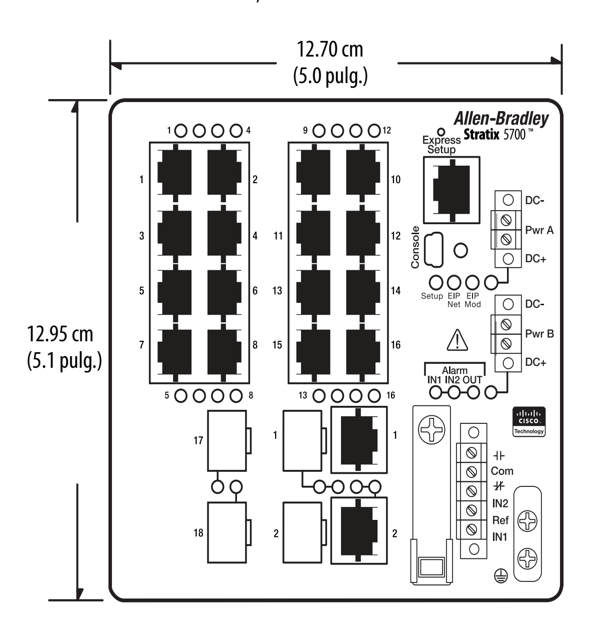
Switches de 10 puertos
1783-BMS10CL, 1783-BMS10CA, 1783-BMS10CGL, 1783-BMS10CGA

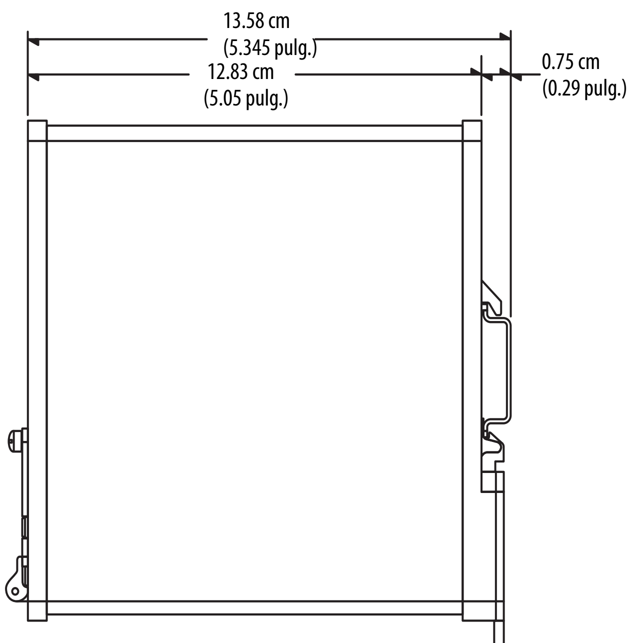


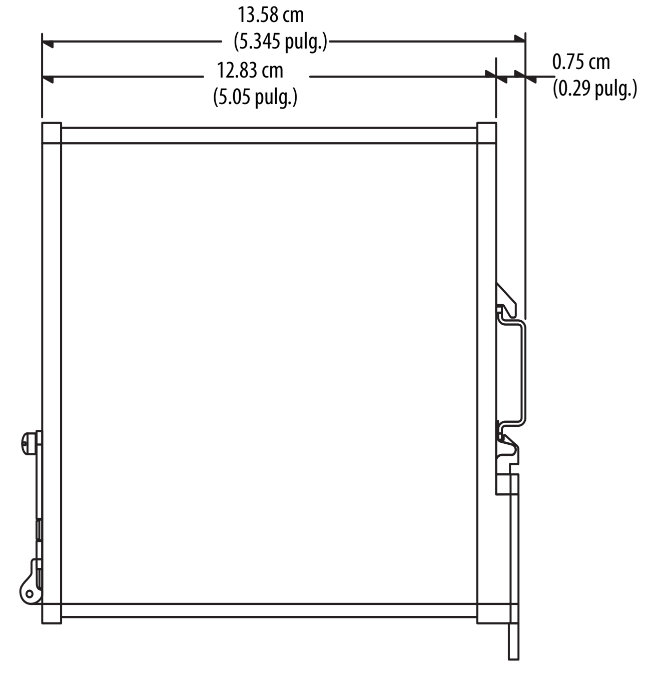
Switch de 10 puertos
1783-BMS10CGP, 1783-BMS10CGN



Switches de 18 y de 20 puertos
1783-BMS12T4E2CGNK, 1783-BMS12T4E2CGP, 1783-BMS12T4E2CGL, 1783-BMS20CL, 1783-BMS20CA, 1783-BMS20CGL, 1783-BMS20CGP, 1783-BMS20CGN, 1783-BMS20CGPK

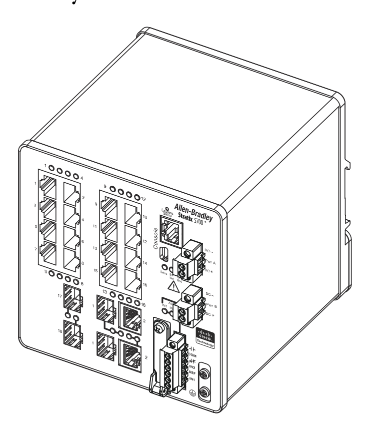






Panel frontal del switch

El panel frontal del switch contiene los puertos, los indicadores de estado y los conectores de alimentación y de relé.



Características de hardware del switch

Estas características de hardware se encuentran disponibles en los switches Stratix 5700.

Característica	Descripción
Conectores de alimentación y de relé	Usted conecta las señales de alimentación CC y de alarma al switch a través de los dos conectores del panel frontal. Un conector proporciona la alimentación de CC primaria (Pwr A) y un segundo conector (Pwr B) proporciona la alimentación secundaria. Los dos conectores son físicamente idénticos y se encuentran en el lado derecho del panel frontal. El conector de alarmas de 6 pines proporciona la interface para un relé de alarma de salida y dos alarmas de entrada. La alarma de salida se puede activar para responder a condiciones de alarma ambientales, de fuente de alimentación y de estado de puertos, y se puede configurar para indicar una alarma con un contacto normalmente abierto y otro normalmente cerrado (formato C). Desde la CLI, puede configurar la alarma de salida para que esté normalmente energizada o normalmente desenergizada. Los terminales de alarma de entrada se pueden utilizar para activar las alarmas en respuesta a cualquier condición externa al switch. El switch puede funcionar con una sola fuente de alimentación o con dos fuentes de alimentación. Cuando ambas fuentes de alimentación están operativas, el switch consume alimentación eléctrica de la fuente de CC con el voltaje más alto. Si falla una de las dos fuentes de alimentación, la otra sigue alimentando al switch.
Puerto de consola	Para configurar, monitorear y administrar el switch, puede conectarlo a una computadora a través del puerto de consola mediante un cable adaptador RJ45 a DB-9 o un cable mini USB (ninguno de estos cables se proporciona con el switch). El driver mini USB se encuentra disponible en la sección de descarga de firmware en http://www.rockwellautomation.com.
Puertos de vínculo ascendente de doble función	Los puertos de vínculo ascendente de doble función disponibles en algunos modelos se pueden configurar individualmente según el tipo de medio físico: RJ45 (cobre) o SFP (fibra). Solo puede haber activa una de estas conexiones a la vez en cada puerto de doble función. Si se conectan ambos puertos, el puerto de módulo SFP tiene prioridad. Puede establecer los puertos RJ45 de cobre para que funcionen a 10, 100 o 1000 Mbps (1000 Mbps no es compatible con todos los módulos con puertos combinados), en modo half-duplex o full-duplex. Puede configurarlos como puertos Ethernet a velocidades fijas de 10, 100 o 1000 Mbps (Gigabit), y puede configurar el modo dúplex. Puede utilizar módulos SFP Ethernet Gigabit (o 100 Mbps) aprobados para establecer conexiones de fibra óptica con otros switches. Estos módulos transceivers se pueden reemplazar en campo y proporcionan las interfaces de vínculo ascendente cuando se insertan en una ranura de módulo SFP. Se utilizan cables de fibra óptica con conectores LC para conectar a un módulo SFP de fibra óptica. Estos puertos funcionan solo en modo full-duplex.
Puertos 10/100	Puede establecer los puertos 10/100 para que funcionen a 10 o 100 Mbps, full-duplex o half-duplex. También puede configurar estos puertos para autonegociación de velocidad y modo dúplex de conformidad con IEEE 802.3-2002. (El ajuste predeterminado es autonegociación). Cuando se configura para autonegociación, el puerto detecta los ajustes de velocidad y modo dúplex del dispositivo conectado. Si el dispositivo conectado también admite autonegociación, el puerto del switch negocia la mejor conexión (es decir, la mayor velocidad de línea que ambos dispositivos admiten y el modo de transmisión full-duplex si el dispositivo conectado lo admite) y se autoconfigura como corresponda. En todos los casos, el dispositivo conectado debe estar a una distancia máxima de 100 m (328 pies) del switch.
Puertos PoE	Los puertos PoE disponibles en algunos modelos pueden configurarse para PoE (IEEE 802.3af) o PoE+ (IEEE 802.3at Tipo 2): • Para configuración PoE, los puertos PoE requieren una fuente de alimentación de entrada externa de 48 VCC de 2 cables. • Para configuración PoE+, los puertos PoE requieren una fuente de alimentación de entrada externa de 54 VCC de 2 cables.
Auto-MDIX	Al conectar el switch a estaciones de trabajo, servidores y encaminadores, normalmente se utilizan cables de tipo directo. No obstante, la característica automática de conexión cruzada de interface dependiente del medio (Auto-MDIX) del switch está habilitada de manera predeterminada y reconfigura automáticamente los puertos para utilizar un cable de tipo directo o cruzado. La característica Auto-MDIX está habilitada de forma predeterminada. Cuando Auto-MDIX está habilitada, el switch detecta el tipo de cable necesario (directo o cruzado) para las conexiones Ethernet de cobre y configura las interfaces como corresponde. Puede utilizar la interface de línea de comandos (CLI) para inhabilitar la característica Auto-MDIX. Consulte la ayuda en línea para obtener más información.

Archivos de configuración

El archivo de configuración del switch (config.txt) tiene un formato ASCII de fácil lectura. Este archivo de configuración se guarda en la memoria no volátil y se escribe en la memoria de acceso aleatorio (RAM) de los switches para usarse como la configuración de funcionamiento cuando se enciende el switch. Cuando se realizan cambios en la configuración, estos cambios tendrán efecto inmediato en la configuración en ejecución. La interface web del administrador de dispositivos y el Add-on Profile (AOP) para la aplicación Logix Designer escriben automáticamente los cambios en la memoria flash para que se conserven para el siguiente ciclo de encendido. Los cambios realizados a través de la CLI deben escribirse manualmente en la memoria flash para que se conserven para el siguiente ciclo de encendido.

Tarjeta SD

El switch está equipado con una ranura para una tarjeta Secure Digital (SD) opcional, además de la memoria flash incorporada. La tarjeta SD se puede utilizar en lugar de la memoria flash incorporada para restaurar fácilmente una configuración del switch en caso de fallo o para duplicar fácilmente configuraciones cuando esté instalando una nueva red.

Si la tarjeta SD está instalada en el switch, el switch inicia el IOS y la configuración presentes en la tarjeta SD. Si la tarjeta SD no está instalada o los archivos no están presentes, el switch lee los parámetros de inicialización incorporados y se reinicia a partir de la imagen del IOS especificada de la memoria flash incorporada.

Debe utilizar la tarjeta SD disponible a través de Rockwell Automation (número de catálogo 1784-SD1) con el switch.



ATENCIÓN: Rockwell Automation se reserva el derecho a denegar la asistencia técnica si se utiliza una tarjeta SD que no es de Rockwell en este producto.

Si realiza el inicio desde la tarjeta SD y, a continuación, la retira mientras el switch está en ejecución, se aplican las siguientes condiciones:

- Ya no será posible acceder a la interface web del administrador de dispositivos.
- Los cambios realizados utilizando la CLI o el AOP entran en vigor, pero no se guardan cuando se reinicia el switch.
- Si la tarjeta SD se reinserta en la ranura, los cambios no se guardan en la tarjeta a menos que se realicen nuevos cambios. A continuación, se guarda toda la configuración en la tarjeta.



ATENCIÓN: Las tarjetas SD normalmente tienen un interruptor que permite su bloqueo para impedir su escritura. Si este interruptor se coloca en la posición de bloqueo, el switch se inicia con éxito usando la tarjeta SD. Los cambios realizados utilizando la CLI, el AOP, o la interface web del administrador de dispositivos surten efecto, pero no se guardan cuando se reinicia el switch.

Sincronización de la tarjeta SD

Puede utilizar la interface web del administrador de dispositivos o el AOP para la aplicación Logix Designer a fin de sincronizar la tarjeta SD para las actualizaciones de la configuración y del IOS. El proceso de sincronización de la configuración sincroniza config.text y vlan.dat entre el origen elegido y el destino elegido.

El proceso de sincronización de la imagen IOS sincroniza la imagen IOS de inicialización existente entre el origen elegido y el destino elegido. Este proceso tarda aproximadamente cinco minutos en completarse.

Si hay otros archivos como, por ejemplo, configuraciones de copias de seguridad, presentes en la tarjeta SD, no se sincronizan.



ATENCIÓN: Cuando realice la sincronización, tenga en cuenta cuál es su origen de inicio, para saber de qué modo hacer la sincronización. El administrador de dispositivos proporciona esta información en la ficha SD Card Sync.
Puede sobrescribir la configuración deseada si realiza la sincronización en la dirección incorrecta.

Asignación de memoria al switch

La tabla siguiente proporciona detalles sobre la asignación de memoria predeterminada para los switches.

Puede utilizar plantillas SDM para configurar los recursos del sistema en el switch a fin de optimizar la compatibilidad con las características específicas, dependiendo de cómo se use el switch en la red. Puede seleccionar una plantilla a fin de proporcionar la máxima utilización del sistema para algunas funciones como, por ejemplo, utilizar la plantilla determinada para equilibrar recursos, y utilizar la plantilla de acceso para lograr la máxima utilización de las ACL. Para asignar recursos de hardware para diferentes usos, las plantillas SDM del switch priorizan los recursos del sistema para optimizar la compatibilidad de determinadas características.

Las siguientes plantillas SDM están disponibles:

- Predeterminada
- Encaminamiento
- IPv4 e IPv6 dobles

Considere utilizar la plantilla de encaminamiento si habilita el encaminamiento estático o si tiene más de 180 IGMP o rutas de multidifusión. Considere utilizar la plantilla de IPv4 e IPv6 dobles si usa IPv6.

Puede seleccionar plantillas SDM para la versión 4 de IP (IPv4) para optimizar estas características.

Característica	Asignación de memoria		
	Predeterminada	Encaminamiento	IPv4 e IPv6 dobles
Direcciones MAC de unidifusión	8 K	4 K	7.5 K
Grupos IGMP IPv4 + rutas de multidifusión	0.25 K	0.25 K	0.25 K
Rutas de unidifusión IPv4	0	4.25 K	0
Grupos de multidifusión IPv6	0	0	0.375 K
Anfitriones IPv4 conectados directamente	0	4 K	
Direcciones IPv6 conectadas directamente	0	0	o
Rutas IPv4 indirectas	0	0.25 K	
Rutas IPv6 indirectas	0	0	0
ACE de encaminamiento basado en políticas IPv4	0	0	
ACE de QoS IPv4/MAC	0.375 K	0.375 K	0.375 K
ACE de seguridad IPv4/MAC	0.375 K	0.375 K	0.375 K
ACE de encaminamiento basado en políticas IPv6	0	0	0
ACE de QOS IPv6	0	0	0
ACE de seguridad IPv6	0	0	0.125 K

Interface web del administrador de dispositivos

Puede administrar el switch utilizando la interface web del administrador de dispositivos para configurar y monitorear el switch. La interface web del administrador de dispositivoses una herramienta de administración de dispositivos gráficos para configurar, monitorear y resolver problemas de switches individuales.

La interface web del administrador de dispositivos muestra vistas en tiempo real de la configuración y el rendimiento del switch. Simplifica las tareas de configuración con características como Smartports para configurar rápidamente el switch y sus puertos. Utiliza pantallas gráficas codificadas por colores, como la vista Front Panel, gráficos e indicadores animados para simplificar las tareas de monitoreo. Proporciona herramientas de alerta para ayudarle a identificar y resolver problemas de la red.

Puede mostrar en pantalla la interface web del administrador de dispositivos desde cualquier parte de su red a través de un navegador web como Microsoft Internet Explorer.

Requisitos de hardware

Atributo	Requisito
Velocidad del procesador	1 GHz o superior (32 bits o 64 bits)
RAM	1 GB (32 bits) o 2 GB (64 bits)
Espacio disponible en disco duro	16 GB (32 bits) o 20 GB (64 bits)
Número de colores	256
Resolución	1024 x 768
Tamaño de fuente	Pequeño

Requisitos de software

navegador web	Versión
Microsoft Internet Explorer	9.0, 10.0 u 11.0 con JavaScript habilitado
Mozilla Firefox	25 o 26 con JavaScript habilitado

La interface web del administrador de dispositivos verifica la versión del navegador cuando se inicia una sesión para asegurarse de que el navegador sea compatible.

SUGERENCIA Para que la interface web del administrador de dispositivos funcione correctamente, inhabilite los bloqueadores de elementos eme-rgentes y los ajustes de proxy en el software de su navegador y los clientes inalámbricos que se estén ejecutando en su computadora personal.

Ambiente Studio 5000

Puede administrar el switch mediante la aplicación Logix Designer en el ambiente Studio 5000. La aplicación Logix Designer cumple con la norma IEC 61131-3 y ofrece editores de lógica de escalera de relés, texto estructurado, diagrama de bloque de funciones y diagrama de funciones secuenciales, para que usted pueda desarrollar programas de aplicaciones.

Requisitos de hardware

Atributo	Requisito
Velocidad del procesador	Pentium II 450 MHz mín. Pentium III 733 MHz (o superior) recomendado
RAM	128 MB mín. 256 MB recomendados
Espacio disponible en disco duro	3 GB
Unidades ópticas	DVD
Requisitos de vídeo	Adaptador de gráficos VGA de 256 colores 800 x 600 de resolución mín. (True Color 1024 x 768 recomendado)
Resolución	800 x 600 de resolución mín. (True Color 1024 x 768 recomendado)

Cisco Network Assistant

Cisco Network Assistant es una interface web que se descarga del sitio web de Cisco y se ejecuta en su computadora. Ofrece opciones avanzadas para configurar y monitorear múltiples dispositivos, incluidos switches, grupos de switches, pilas de switches, encaminadores y puntos de acceso.

Para utilizar el software, siga estos pasos.

1. Vaya a http://www.cisco.com/go/NetworkAssistant.

   Debe ser un usuario registrado, pero no necesita otros privilegios de acceso.
2. Localice el instalador de Network Assistant.
3. Descargue el instalador de Network Assistant y ejecútelo.

   Puede ejecutarlo directamente desde la web si su navegador ofrece esta opción.
4. Cuando ejecute el instalador, siga las instrucciones que se muestran.
5. En el panel final, haga clic en Finish para completar la instalación de Network Assistant.
6. Consulte la ayuda en línea de Network Assistant para obtener más información.

Interface de línea de comandos

Puede administrar el switch desde la interface de línea de comandos (CLI), para lo cual debe conectar su computadora personal directamente al puerto de la consola del switch o a través de la red utilizando Telnet.

Para obtener acceso a la CLI mediante el puerto de la consola, siga estos pasos.

1. Conéctese con el puerto de la consola en una de estas formas:
   - Utilice un cable adaptador RJ45 a DB-9 (no suministrado con el switch) para conectarse con el puerto serial de 9 pines estándar en una computadora personal.
   - Utilice un cable mini USB estándar (no suministrado con el switch) para conectarse con el puerto mini USB en una computadora personal.
   - Si va a utilizar el cable USB, descargue los drivers para su computadora equipada con Microsoft Windows de http://www.rockwellautomation.com.
2. Conecte el otro extremo del cable al puerto de la consola en el switch.



ADVERTENCIA: El puerto de la consola está concebido solamente para programación local temporal, no para conexión permanente. Si conecta o desconecta el cable de la consola con la alimentación aplicada a este módulo o al dispositivo de programación en el otro extremo del cable, se puede producir un arco eléctrico. Esto puede causar una explosión en instalaciones ubicadas en zonas peligrosas. Antes de seguir adelante, asegúrese de desconectar la alimentación eléctrica o de verificar que la zona no sea peligrosa.

3. Inicie un programa de emulación de terminal en la computadora personal.
4. Configure el software de emulación de terminal de la computadora personal para que funcione a 9600 bps, 8 bits de datos, sin paridad, 1 bit de parada y sin control de flujo.

Notas:

Instalación del switch

Pautas de instalación



ATENCIÓN: Este equipo es adecuado únicamente para uso en zonas Clase I, División 2, Grupos A, B, C, D o en zonas no peligrosas.



Al final de su vida útil, este equipo no debe desecharse en la basura municipal general.

Cuando determine la ubicación del switch, siga estas pautas:

- El flujo de aire alrededor del switch no debe estar restringido. Para impedir el sobrecalentamiento del switch, observe las siguientes indicaciones sobre el espacio libre:
  - Por arriba y por debajo: 50.8 mm (2.0 pulg.)
  - Por los lados: 50.8 mm (2.0 pulg.)
  - Parte frontal: 50.8 mm (2.0 pulg.)
- Para puertos 10/100 y puertos 10/100/1000, la longitud del cable desde un switch hasta un dispositivo conectado no puede exceder los 100 metros (328 pies).
- La longitud del cable de fibra óptica desde un switch hasta un dispositivo conectado no puede exceder la distancia especificada en el Apéndice C.
- Para lograr la máxima inmunidad al ruido, deben usarse cables apantallados en los puertos de vínculos ascendentes RJ45 (Gi1/1 y Gi1/2) de estos switches:
  - 1783-BMS06TGL
  - 1783-BMS06TGA
  - 1783-BMS10CGL
  - 1783-BMS10CGA
  - 1783-BMS10CGN
  - 1783-BMS10CGP
  - 1783-BMS12T4E2CGNK
  - 1783-BMS12T4E2CGP
  - 1783-BMS12T4E2CGL
  - 1783-BMS20CGL
  - 1783-BMS20CGN
  - 1783-BMS20CGP
  - 1783-BMS20CGPK
- La temperatura alrededor de la unidad no debe exceder los 60 °C (140 °F).

IMPORTANTE Cuando el switch se instala en un envolvente industrial, la temperatura en el interior del envolvente es superior a la temperatura ambiente normal en el exterior del envolvente.

La temperatura en el interior del envolvente no puede ser superior a 60 °C (140 °F), que es la temperatura ambiente máxima del switch.

- El espacio libre hasta los paneles frontal y posterior cumple estas condiciones:
  - Los indicadores de estado del panel frontal se pueden leer fácilmente.
  - El acceso a los puertos es suficiente para un cableado sin restricciones.
  - Los conectores de alimentación de corriente continua (CC) del panel frontal y el conector del relé de alarma quedan dentro del alcance de la conexión con la fuente de alimentación de CC.
- El cableado está lejos de las fuentes de ruido eléctrico, como radios, líneas de alimentación eléctrica y unidades de iluminación fluorescente.
- Conecte la unidad únicamente a una fuente de alimentación de CC Clase 2.

Instale o retire la tarjeta SD (opcional)

Para instalar o sustituir la tarjeta SD, siga estos pasos.

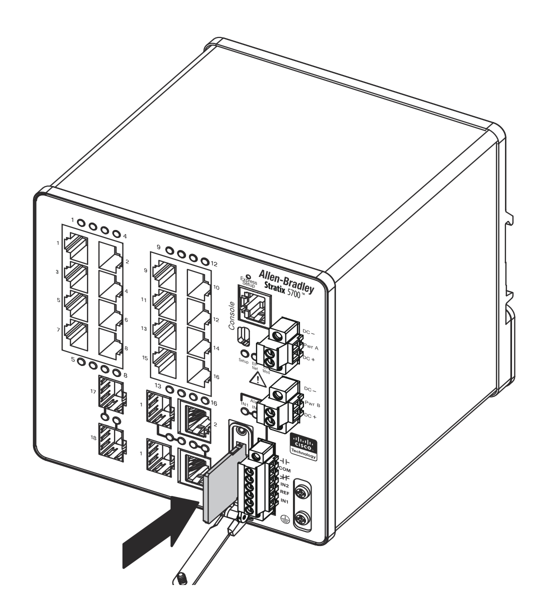
1. En la parte frontal del switch, localice la puerta que protege la ranura para tarjetas SD.
2. Afloje con un destornillador el tornillo prisionero de cabeza moleteada situado en la parte superior de la puerta para abrir la puerta.
   a. Para instalar una tarjeta, deslícela hacia el interior de la ranura y presiónela firmemente en su sitio hasta que quede bloqueada por el mecanismo accionado por resorte.

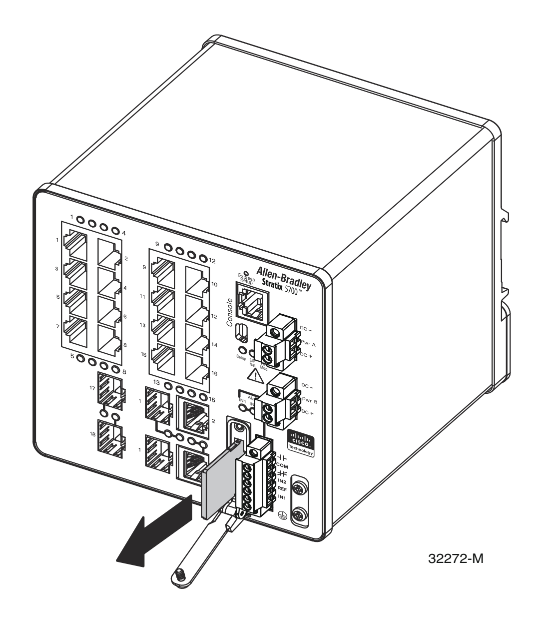
      La tarjeta está codificada para evitar que pueda ser totalmente insertada de manera incorrecta.

   b. Para retirar la tarjeta, empújela hacia dentro y déjela emerger mediante el mecanismo accionado por resorte.

   c. Sujete la tarjeta por la parte superior y tire de ella hacia fuera.

      Colóquela en una bolsa antiestática para protegerla de descargas electrostáticas.





3. Una vez instalada la tarjeta, cierre la puerta de guarda y apriete el tornillo prisionero con un destornillador para fijar la puerta en su sitio.

Verifique el funcionamiento del switch

Antes de instalar el switch en su ubicación final, enciéndalo y verifique si recibe alimentación eléctrica.

El tiempo necesario para que el switch se ponga en marcha está directamente relacionado con la configuración del mismo. El tiempo de inicio puede verse afectado negativamente por lo siguiente:

- El modo Spanning Tree Learning
- El número de archivos o imágenes en la memoria flash incorporada

Para probar el switch, siga estos pasos.

1. Encienda el switch.

   Para suministrar alimentación a un switch que está conectado directamente a una fuente de alimentación de CC, localice el disyuntor en el panel que alimenta al circuito de CC y coloque el disyuntor en la posición ON.

2. Verifique la secuencia de puesta en marcha.

   Cuando encienda el switch, comenzará automáticamente una rutina rápida de arranque. El indicador de estado del sistema parpadeará de color verde cuando se cargue la imagen del software IOS. Si falla la rutina, el color del indicador de estado del sistema cambiará a rojo.



ATENCIÓN: Los fallos durante la puesta en marcha suelen ser fatales para el switch. Comuníquese inmediatamente con el representante de Rockwell Automation si el switch no finaliza correctamente la secuencia de puesta en marcha.

IMPORTANTE Puede inhabilitar la inicialización rápida y ejecutar la autoprueba de encendido (POST) mediante la CLI del IOS. Consulte la documentación correspondiente en http://www.Cisco.com para obtener más información.

3. Después de realizar esta prueba correctamente, haga lo siguiente:
   a. Desactive la alimentación eléctrica del switch.
   b. Desconecte los cables.
   c. Decida dónde desea instalar el switch

Conecte la tierra de protección y la alimentación de CC

En estas secciones se describen los pasos necesarios para conectar una tierra de protección y la alimentación de CC al switch.

Para las conexiones de alimentación de CC, use un cable AWM (material de cableado para aparatos) de cobre en forma de par trenzado, estilo 1007 o 1569, con clasificación UL y CSA, como el número de pieza 9318 de Belden.

Puesta a tierra del switch



ATENCIÓN: Este equipo debe estar conectado a tierra. No anule nunca el conductor de tierra ni ponga en marcha el equipo sin contar con un conductor de conexión a tierra correctamente instalado. Comuníquese con la autoridad de inspección eléctrica pertinente o con un electricista si no sabe con seguridad si hay una conexión de tierra apropiada disponible.

Este equipo está diseñado para estar conectado a tierra a fin de cumplir los requisitos de emisiones e inmunidad. Asegúrese de que el terminal de conexión a tierra funcional del switch esté conectado a tierra durante el funcionamiento normal.



ATENCIÓN: Para asegurarse de que el equipo tenga una conexión fiable a tierra física, siga las instrucciones del procedimiento de puesta a tierra y use un terminal de anillo UL Listed adecuado para cables números 10 a 12 AWG como, por ejemplo, el terminal Thomas & Betts identificado con el número de pieza 10RCR, o uno equivalente.

Use cable de un calibre no menor que 12 AWG (4 mm^2) para conectarlo al tornillo de puesta a tierra externo.

El terminal de conexión a tierra no se suministra con el switch. Puede utilizar una de estas opciones:
- Terminal de un solo anillo
- Dos terminales de un solo anillo

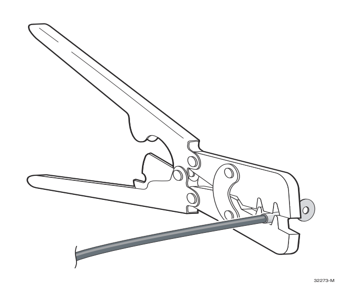
Para conectar el switch a tierra física, siga estos pasos. Asegúrese de seguir los requisitos de puesta a tierra del sitio de instalación.

1. Utilice un destornillador Phillips o un destornillador de trinquete con punta Phillips para sacar los tornillos de puesta a tierra del panel frontal del switch.

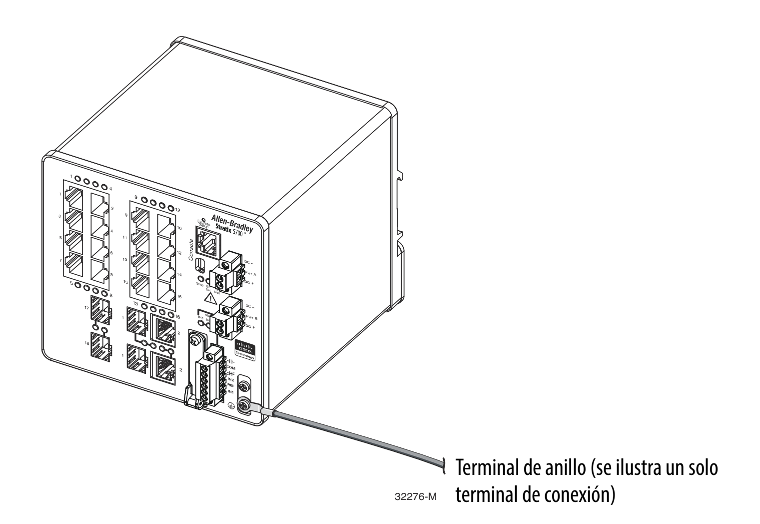
   Guarde el tornillo de tierra para utilizarlo posteriormente.
2. Siga las pautas del fabricante para determinar la longitud de cable que se debe pelar.

3. Inserte el cable de tierra en el terminal de anillo y utilice una herramienta de engarzado para engarzar el terminal en el cable.

   Si va a usar dos terminales de anillo, repita esta acción con el segundo terminal de anillo.



4. Haga pasar el tornillo de tierra a través del terminal.
5. Inserte el tornillo de tierra en la abertura para el tornillo de tierra funcional ubicada en el panel frontal.



6. Utilice un destornillador de trinquete para apretar los tornillos de tierra y los terminales de anillo al panel frontal del switch a 0.4 N•m (3.5 lb•pulg.).

   No exceda el par de apriete recomendado.

7. Conecte el otro extremo del cable de tierra a una superficie metálica sin recubrimiento conectada a tierra como, por ejemplo, un bus de tierra, un riel DIN conectado a tierra o un rack sin recubrimiento conectado a tierra.

Cablee la fuente de alimentación de CC del switch

Siga estos pasos para cablear la fuente de alimentación de CC del switch.



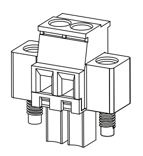
ATENCIÓN: Antes de realizar cualquiera de los siguientes procedimientos, asegúrese de que la alimentación eléctrica esté desconectada del circuito de CC o de que el área se considere no peligrosa antes de continuar:

- Este producto está concebido para recibir alimentación eléctrica de una fuente de alimentación Clase 2 marcada como "Class 2" y con un voltaje nominal de 12, 24 o 48 VCC, 2.5 A.
- Para satisfacer la directiva de bajo voltaje (LVD) de la CE, este equipo debe recibir la alimentación de una fuente que cumpla los requisitos de voltaje de seguridad extrabajo (SELV) o voltaje de protección extrabajo (PELV).
- Se debe incorporar un dispositivo de desconexión de dos polos de fácil acceso en el cableado fijo.
- Este producto depende de la instalación del edificio para la protección contra cortocircuitos (sobrecorriente). Asegúrese de que la clasificación del dispositivo de protección no sea superior a 3 A.
- La instalación del equipo debe satisfacer los códigos eléctricos locales y nacionales.
- Las tareas de instalación, reemplazo o reparación de este equipo solo podrán ser realizadas por personal debidamente capacitado y cualificado.



ATENCIÓN: Para las conexiones de los cables al conector de alimentación eléctrica y del relé, use cable AWM (material de cableado para aparatos) de cobre en forma de par trenzado, estilo 1007 o 1569, con clasificación UL y CSA (como el número de pieza 9318 de Belden).

1. Localice el conector de alimentación eléctrica.



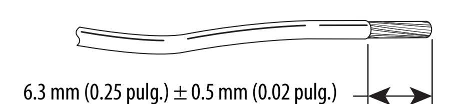
2. Identifique las conexiones de alimentación eléctrica de CC positiva y de retorno.

   La conexión de corriente CC positiva está rotulada DC+, y la conexión de corriente CC negativa es la adyacente, rotulada DC-.

3. Mida un tramo de cable de cobre de 0.82…0.52 mm^2 (18…20 AWG) suficientemente largo para permitir la conexión con la fuente de alimentación de CC.

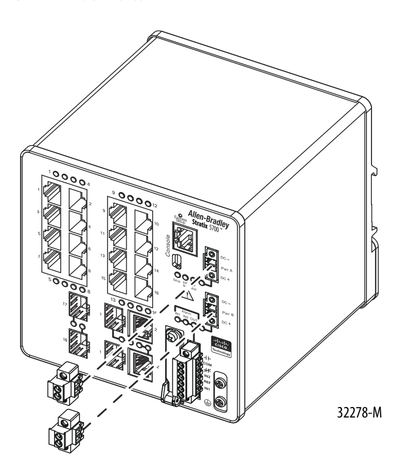
4. Mediante un pelacables de calibre 18, pele un tramo de 6.3 mm (0.25 pulg.) ± 0.5 mm (0.02 pulg.) de cada uno de los dos cables.

   No pele más de 6.8 mm (0.27 pulg.) de aislamiento del cable. Si se pela una cantidad de cable mayor que la recomendada, es posible que quede cable expuesto tras la instalación.



5. Afloje los dos tornillos prisioneros que conectan el conector de alimentación eléctrica al switch y retire el conector de alimentación eléctrica.

   Retire los dos conectores si va a realizar la conexión a dos fuentes de alimentación eléctrica.

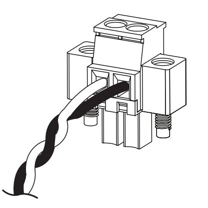


6. Inserte la parte expuesta del cable positivo en la conexión rotulada DC+ y la parte expuesta del cable de retorno en la conexión rotulada DC-.

   Asegúrese de que no se vea el conductor del cable por ninguna parte. Solo se puede ver cable con aislamiento saliendo del conector.

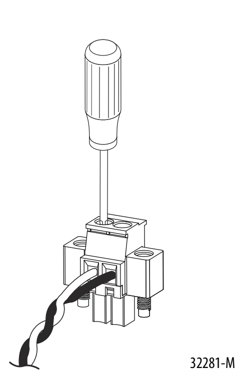


ATENCIÓN: Un conductor de cable expuesto de una fuente de alimentación de entrada de CC puede conducir niveles peligrosos de electricidad. Asegúrese de que ninguna parte expuesta del cable de la fuente de alimentación de entrada de CC sobresalga de los conectores o bloques de terminales.



7. Utilice un destornillador de trinquete para apretar los tornillos prisioneros del conector de alimentación (encima de los conductores del cable instalado) a 0.23 N•m (2.0 lb•pulg.).

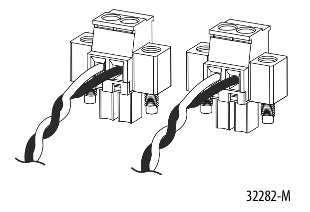
   No exceda el par de apriete recomendado.



8. Conecte el otro extremo del cable positivo al terminal positivo de la fuente de alimentación de CC, y conecte el otro extremo del cable de retorno al terminal de retorno de la fuente de alimentación de CC.

   Cuando pruebe el switch, bastará con usar una sola conexión de alimentación. Si va a instalar el switch y usa una segunda fuente de alimentación, repita este procedimiento con el segundo conector de alimentación eléctrica.

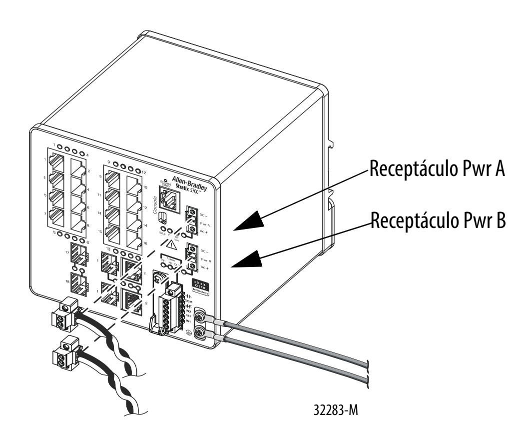
   En la figura siguiente se muestra el cableado finalizado de una entrada de CC al conector de una fuente de alimentación primaria y una fuente de alimentación secundaria opcional.



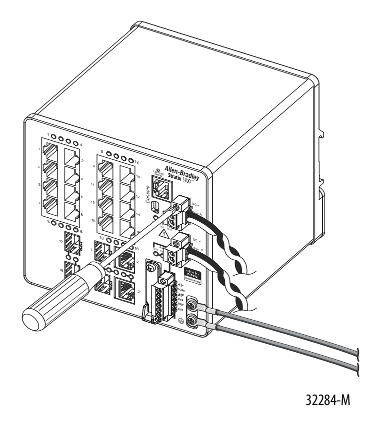
Conecte los conectores de alimentación del switch

Para conectar los conectores de alimentación del switch al panel frontal del switch, siga estos pasos.

1. Inserte un conector de alimentación en el receptáculo Pwr A del panel frontal del switch, y el otro en el receptáculo Pwr B.



2. Use a destornillador plano de trinquete para apretar los tornillos prisioneros situados a los lados de los conectores de alimentación.



   Cuando pruebe el switch, bastará con usar una sola fuente de alimentación. Si va a instalar el switch y usa una segunda fuente de alimentación, repita este procedimiento con el segundo conector de alimentación (Pwr B), que se instala justo debajo del conector de la fuente de alimentación primaria (Pwr A).

3. Cuando vaya a instalar el switch, fije al rack los cables procedentes de los conectores de alimentación mediante bridas.

Cablee la fuente de CC para alimentación a través de Ethernet (opcional)

Este procedimiento se aplica solo a los switches con puertos PoE.



ADVERTENCIA: El puerto de la consola está concebido solamente para programación local temporal, no para conexión permanente. Si conecta o desconecta el cable de la consola con la alimentación aplicada a este módulo o al dispositivo de programación en el otro extremo del cable, se puede producir un arco eléctrico. Esto puede causar una explosión en instalaciones ubicadas en zonas peligrosas. Antes de seguir adelante, asegúrese de desconectar la alimentación eléctrica o de verificar que la zona no sea peligrosa.



ATENCIÓN: Para satisfacer la directiva de bajo voltaje (LVD) de la CE, este equipo debe recibir la alimentación de una fuente que cumpla los requisitos de voltaje de seguridad extrabajo (SELV) o voltaje de protección extrabajo (PELV).

Para cumplir las restricciones de UL, este equipo debe recibir la alimentación de una fuente que cumpla los requisitos de la clase 2 o voltaje/corriente limitados.

El switch debe estar cableado y conectado a tierra.

Los requisitos de la fuente de alimentación eléctrica dependen de la aplicación.

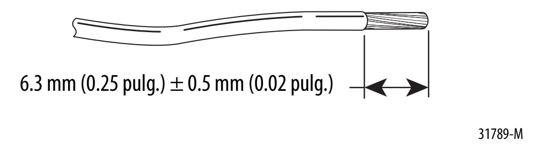
Aplicación	Suministro de energía por puerto	Consumo de energía	Productos Allen-Bradley
Solo PoE IEEE 802.3af	44…57 VCC (48 VCC nom.)	15.4 W, máx.	Fuentes de alimentación eléctrica conmutadas: • 1606-XL Standard • 1606-XLE Essential • 1606-XLP Compact • 1606-XLS Performance
PoE y PoE + IEEE 802.3at Tipo 2	50…57 VCC (54 VCC nom.)	15.4 W, máx. para PoE 30 W, máx. para PoE+	



ADVERTENCIA: Antes de realizar cualquiera de los siguientes procedimientos, asegúrese de que la alimentación eléctrica esté desconectada del circuito de CC o de que el área se considere no peligrosa antes de continuar:

1. Mida un tramo de cable de cobre de 0.82...0.52 mm^2 (18...20 AWG) suficientemente largo para permitir la conexión con la fuente de alimentación de CC.
2. Mediante un pelacables de calibre 18, pele un tramo de 6.3 mm (0.25 pulg.) ± 0.5 mm (0.02 pulg.) de cada uno de los dos cables.

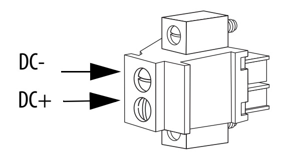
   No pele más de 6.8 mm (0.27 pulg.) de aislamiento del cable. Si se pela una cantidad de cable mayor que la recomendada, es posible que quede cable expuesto tras la instalación.



3. Localice el conector de alimentación eléctrica.

4. Inserte la parte expuesta del cable positivo en la conexión rotulada DC+ y la parte expuesta del cable de retorno en la conexión rotulada DC-.

   Asegúrese de que no puede ver ningún cable desnudo. Solo se puede ver cable con aislamiento saliendo del conector.



5. Utilice un destornillador de trinquete para apretar los tornillos prisioneros del conector de alimentación (encima de los conductores del cable instalado) a 0.23 N•m (2.0 lb•pulg.).

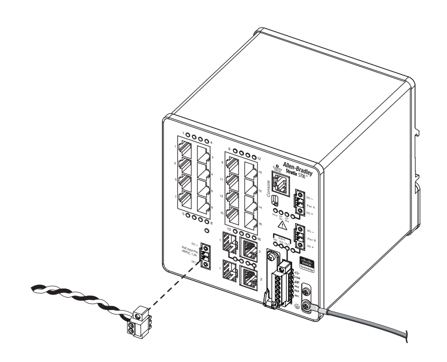
6. Conecte el otro extremo del cable positivo (el que está conectado a DC+) al terminal positivo en la fuente de alimentación de CC, y conecte el otro extremo del cable de retorno (el que está conectado a DC-) al terminal de retorno en la fuente de alimentación de CC.



ATENCIÓN: Si se utilizan varias fuentes de alimentación eléctrica, no debe excederse el voltaje de aislamiento especificado.

Conecte el conector de alimentación PoE (opcional)

1. Inserte el conector de alimentación en el bloque de terminales de entrada de CC del panel frontal del switch.
2. Utilice un destornillador para apretar los tornillos prisioneros a los lados del conector de alimentación.





ATENCIÓN: La exposición a ciertos productos químicos puede degradar las propiedades de sellado de los materiales usados en los relés. Inspeccione periódicamente el relé para determinar si presenta signos de degradación.

Instale el switch

En esta sección se describe la instalación del switch.



ATENCIÓN: Este equipo se suministra como equipo de tipo abierto. Se debe montar dentro de un envolvente con el diseño adecuado para esas condiciones ambientales específicas y estar apropiadamente diseñado para evitar lesiones personales durante el acceso a piezas energizadas. Solo se debe obtener acceso al interior del envolvente mediante una herramienta.

El envolvente debe cumplir los requisitos de clasificación mínimos para envolventes IP 54 o NEMA tipo 4.



ATENCIÓN: Para impedir el sobrecalentamiento del switch, asegúrese de que se observen las siguientes especificaciones de espacio libre:

- Parte superior e inferior: 50.8 mm (2.0 pulg.)
- Lado expuesto (no conectado al módulo): 50.8 mm (2.0 pulg.)
- Parte frontal: 50.8 mm (2.0 pulg.)

Instale el switch en un riel DIN

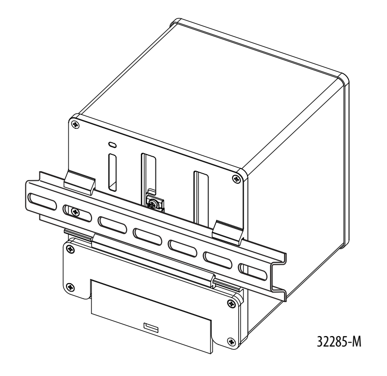
El switch se envía con un sujetador accionado por resorte en el panel posterior para montaje en un riel DIN.



ATENCIÓN: Cuando se utiliza un montaje en riel DIN, también se consigue una puesta a tierra adicional mediante la conexión del riel DIN a la tierra de chasis. Utilice un riel DIN de acero bicromatado para contribuir a una adecuada puesta a tierra. El uso de rieles DIN fabricados con otros materiales (por ejemplo, aluminio o plástico) que puedan sufrir oxidación o corrosión, o que no sean buenos conductores, puede ocasionar una puesta a tierra inadecuada. Asegure el riel DIN a la superficie de montaje aproximadamente cada 200 mm (7.8 pulg.) mediante dispositivos de anclaje de extremos de la manera adecuada y empleando una arandela plana a lo largo de todo el riel DIN.

Para acoplar el switch a un riel DIN, siga estos pasos.

1. Coloque el panel posterior del switch justo frente al riel DIN y asegúrese de que el riel DIN encaja en el espacio entre los dos ganchos situados junto a la parte superior del switch y el sujetador accionado por resorte junto a la parte inferior.
2. Mientras mantiene la parte inferior del switch alejada del riel DIN, coloque los dos ganchos de la parte posterior del switch sobre la parte superior del riel DIN.

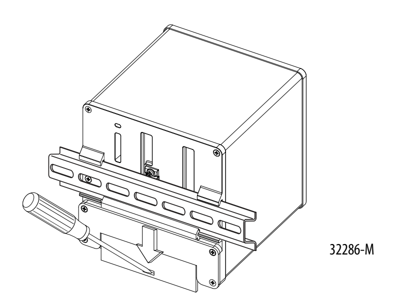


3. Empuje el switch hacia el riel DIN para que el sujetador accionado por resorte de la parte trasera inferior del switch baje y se encaje en su sitio.

Retire el switch del riel DIN

Para retirar el switch de un riel DIN o un rack, siga estos pasos.

1. Corte la alimentación del switch y desconecte todos los cables y conectores del panel frontal del switch.
2. Inserte una herramienta como, por ejemplo, un destornillador plano, en la ranura de la parte inferior del sujetador accionado por resorte y utilícela para soltar el sujetador del riel DIN.



3. Retire el switch del riel DIN.

Instale un módulo SFP (opcional)

En los números de catálogo del switch que admiten comunicaciones por cable de fibra óptica, los módulos SFP se insertan en ranuras para módulos SFP situados en la parte frontal del switch. Estos módulos reemplazables en campo proporcionan interfaces ópticas de vínculo ascendente: envío (TX) y recepción (RX).

Puede usar cualquier combinación de módulos SFP robustos. Cada módulo SFP debe ser del mismo tipo que el módulo SFP situado en el otro extremo del cable. El cable no debe exceder la longitud de cable estipulada para mantener la fiabilidad de las comunicaciones.

Cuando use módulos SFP comerciales, como CWDM y 1000BX-U/D, reduzca la temperatura de funcionamiento máxima en 15 °C (59 °F). La temperatura de funcionamiento mínima es de 0 °C (32 °F).

Para obtener instrucciones detalladas sobre cómo instalar, retirar y cablear el módulo SFP, consulte la documentación del módulo SFP.



ATENCIÓN: Se recomienda encarecidamente no instalar ni retirar el módulo SFP con cables de fibra óptica conectados porque los cables, el conector del cable o las interfaces ópticas del módulo SFP podrían sufrir daños. Desconecte todos los cables antes de retirar o instalar un módulo SFP.

IMPORTANTE La instalación y extracción de un módulo SFP pueden acortar su vida útil. No retire o inserte módulos SFP con más frecuencia de la absolutamente necesaria.

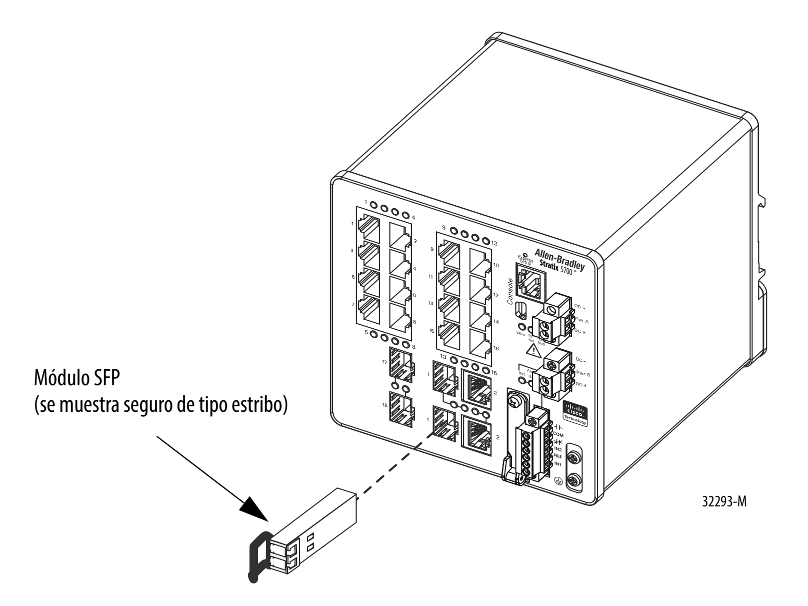
Para insertar un módulo SFP en la ranura para módulos SFP, siga estos pasos.

1. Póngase una muñequera antiestática en la muñeca y conéctela a una superficie metálica sin recubrimiento conectada a tierra.
2. Sujete ambos lados del módulo SFP y alinéelo de lado frente a la abertura de la ranura.



ATENCIÓN: Si el módulo SFP no se puede insertar completamente, deténgase. No fuerce la inserción del módulo en la ranura. Gire el módulo SFP 180° y pruebe de nuevo.

3. Inserte el módulo SFP en la ranura, como se muestra en la figura siguiente, hasta que note que el conector del módulo encaje en su sitio en la parte posterior de la ranura.



4. Retire los tapones antipolvo de los puertos ópticos del módulo SFP y guárdelos para usarlos más adelante.

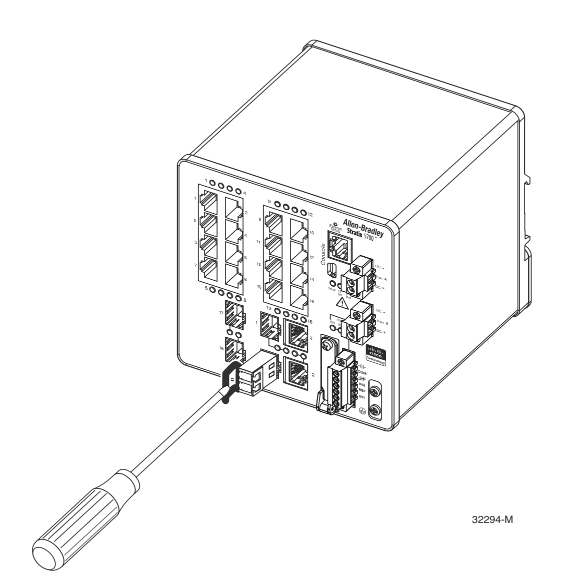
IMPORTANTE	No retire los tapones antipolvo del puerto del módulo SFP ni las tapas de caucho del cable de fibra óptica hasta que esté listo para conectar el cable. Los tapones y tapas protegen los puertos y cables del módulo SFP frente a la contaminación y la luz ambiental.

Retire los módulos SFP de las ranuras para módulos SFP

Para retirar un módulo SFP de un receptáculo para módulos, siga estos pasos.

1. Póngase una muñequera antiestática en la muñeca y conéctela a una superficie metálica sin recubrimiento conectada a tierra.
2. Desconecte el conector LC de fibra del módulo SFP.
3. Inserte un tapón antipolvo en los puertos ópticos del módulo SFP para mantener limpias las interfaces ópticas.
4. Desbloquee y retire el módulo SFP.

   Si el módulo tiene un seguro de tipo estribo, gire el seguro hacia usted y tire suavemente de él para extraer el módulo. Si se obstruye el seguro de tipo estribo y no puede usar el dedo índice para abrirlo, use un destornillador pequeño de punta plana u otro instrumento largo y estrecho para abrir el seguro.



5. Sujete el módulo SFP con los dedos pulgar e índice y sáquelo con cuidado de la ranura para módulos.
6. Coloque el módulo SFP retirado en una bolsa antiestática u otro entorno protector.

Cablee las alarmas externas

El switch tiene dos circuitos de relé de entrada de alarma y un circuito de relé de salida de alarma con formato C (un polo dos posiciones) para las alarmas externas. Los circuitos de relé de alarma de entrada se han diseñado para detectar si la entrada de alarma está abierta o cerrada con respecto al pin de referencia de la entrada de alarma. El circuito de relé de alarma de salida tiene un solo relé con formato C, con un contacto normalmente abierto (N.A.) y otro normalmente cerrado (N.C.). Puede configurar el relé de alarma de salida como normalmente energizado o normalmente desenergizado mediante la CLI.

Consulte en el Apéndice C el ejemplo de cableado de alarma.

Las señales de alarma se conectan al switch mediante el conector del relé de alarma de 6 vías. Hay tres conexiones dedicadas para los dos circuitos de entrada de alarma:

- Entrada de alarma 1 (IN1)
- Entrada de alarma 2 (IN2)
- Tierra de referencia aislada

La conexión del cableado de una entrada de alarma y la tierra de referencia son necesarias para completar un circuito de alarma de una sola entrada. Debe proporcionar un contacto seco N.A. o N.C. para completar el circuito de alarma entre la tierra de referencia e IN1 o IN2.



ATENCIÓN: No aplique una fuente de voltaje externa a las entradas de alarma IN1 o IN2. Limite el cableado de salida de alarma a 48 VCC, 0.5 A.

Las tres conexiones restantes del circuito de alarma de salida con formato C son las siguientes:

- salida N.A.
- salida N.C.
- comunes

Se necesita la conexión del cableado de una salida de alarma y el común para completar un solo circuito de alarma de salida. El relé de salida de alarma con formato C proporciona dos contactos secos: uno N.A. y uno N.C.



ATENCIÓN: Para las conexiones de los cables al conector de alimentación eléctrica y del relé, debe usarse cable AWM (material de cableado para aparatos) de cobre en forma de par trenzado, estilo 1007 o 1569, con clasificación UL y CSA (como el número de pieza 9318 de Belden).

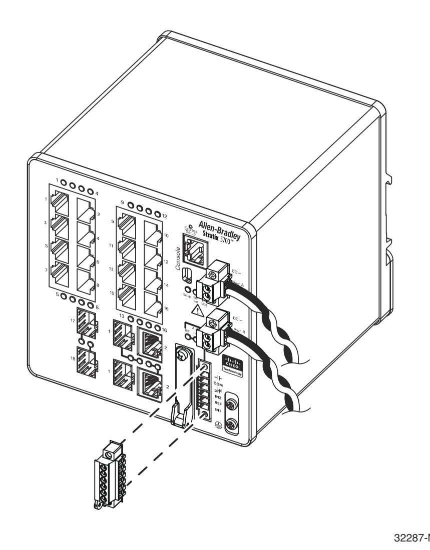
Los rótulos del conector del relé de alarma se encuentran en el panel del switch.

Tabla 1 - Rótulos del conector del relé de alarma

Rótulo	Conexión
NO	Conexión de salida de alarma normalmente abierta (N.A.)
COM	Conexión común de salida de alarma
NC	Conexión de salida de alarma normalmente cerrada (N.C.)
IN2	Entrada de alarma 2
REF	Conexión de tierra de referencia de entrada de alarma
IN1	Entrada de alarma 1

Para cablear el switch a un dispositivo de alarma externo, siga estos pasos.

1. Afloje los tornillos prisioneros que sujetan el conector del relé de alarma del switch y retire el conector del chasis del switch.



2. Mida dos hilos de cable de par trenzado (18…20 AWG) con una longitud suficiente para conectarlos al dispositivo de alarma externo.

   Elija entre configurar un circuito de salida o de entrada de alarma externa.

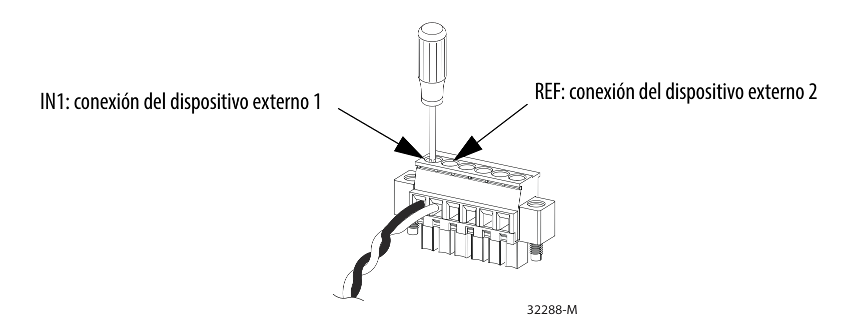
3. Use un pelacables para retirar 6.3 mm (0.25 pulg.) ± 0.5 mm (0.02 pulg.) de aislamiento de ambos extremos de cada cable.

   No pele más de 6.8 mm (0.27 pulg.) de aislamiento de los cables. Si se pela una cantidad de cable mayor que la recomendada, es posible que quede cable expuesto en el conector del relé de alarma tras la instalación.

4. Inserte los cables expuestos del dispositivo de alarma externo en las conexiones en función de la configuración del circuito de entrada o salida de alarma. Consulte la Tabla 1 en la página 44.

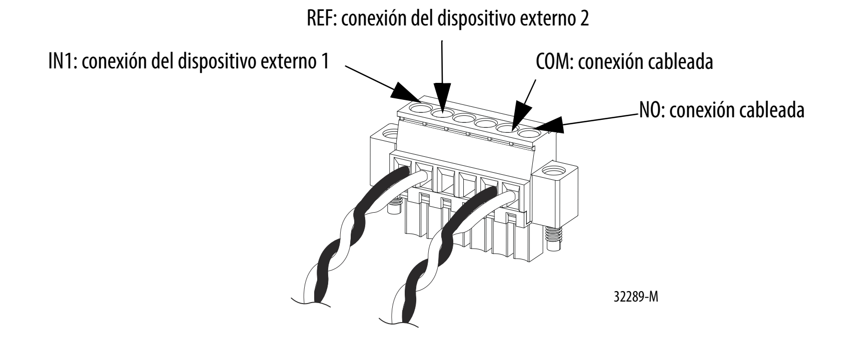
5. Use un destornillador plano de trinquete para apretar el tornillo prisionero del conector del relé de alarma (encima de los conductores de cable instalados) a 0.23 N•m (2.0 lb•pulg.).

   No exceda el par de apriete recomendado.



6. Repita el procedimiento anterior para insertar los cables de entrada y salida de un dispositivo de alarma externo adicional en el conector del relé de alarma.

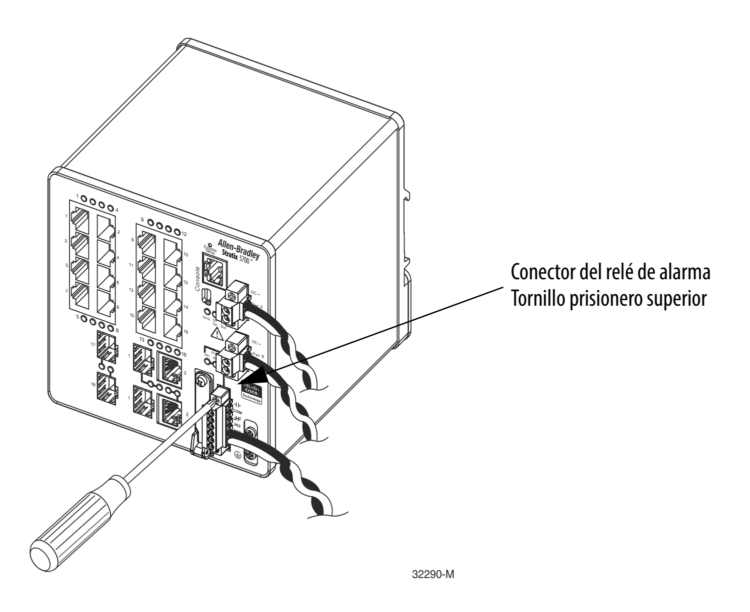
   En la figura siguiente se muestra el cableado finalizado de los dos dispositivos de alarma externos. El primer circuito del dispositivo de alarma está cableado como un circuito de entrada de relé de alarma; las conexiones IN1 y REF completan el circuito. El segundo circuito del dispositivo de alarma está cableado como un circuito de relé de salida de alarma mediante el lado normalmente abierto de los contactos de relé con formato C. Las conexiones NO y COM completan el circuito.



Conecte el conector del relé de alarma al switch

Para conectar el conector del relé de alarma al panel frontal del switch, siga estos pasos.

1. Inserte el conector del relé de alarma al receptáculo del panel frontal del switch.
2. Use un destornillador plano de trinquete para apretar los tornillos prisioneros situados a los lados del conector del relé de alarma.



Conecte los puertos de destino

Para conectar los puertos de destino, siga estos procedimientos.

Conecte a puertos 10/100 y 10/100/1000

Los puertos 10/100/1000 del switch se configuran automáticamente para funcionar a las velocidades de los dispositivos conectados. Si los puertos conectados no admiten autonegociación, puede establecer explícitamente los parámetros de velocidad y dúplex. La conexión de dispositivos que no admitan autonegociación o que tengan los parámetros de velocidad y dúplex establecidos manualmente puede reducir el rendimiento o impedir que se realice la conexión.

La característica Auto-MDIX está habilitada de forma predeterminada. A menos que esta característica esté inhabilitada, puede usar cables directos o cables cruzados para conectar los otros dispositivos de la red.

Para maximizar el rendimiento, elija uno de estos métodos para configurar los puertos Ethernet:

- Deje que los puertos autonegocien la velocidad y el modo dúplex.
- Establezca los parámetros de velocidad y dúplex de los puertos en ambos extremos de la conexión

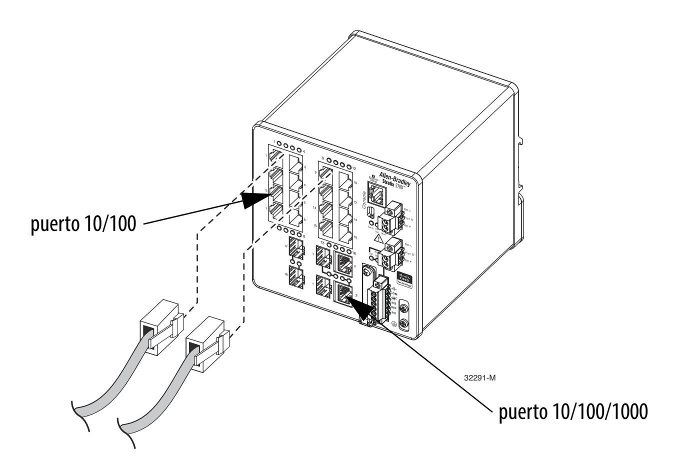
Conecte puertos 10BASE-T, 100BASE-TX o 1000BASE-T

Para conectar puertos 10BASE-T, 100BASE-TX o 1000BASE-T, siga estos pasos.



ATENCIÓN: Para evitar que se produzcan daños por descargas electrostáticas (ESD), siga los procedimientos recomendados sobre el manejo de tarjetas y componentes.

1. Elija una de estas opciones para conectar un dispositivo:
   - Para conectar estaciones de trabajo, servidores y encaminadores, conecte un cable de tipo directo a un conector RJ45 del panel frontal.
   - Al conectar dispositivos compatibles con 1000BASE-T, use un cable con cuatro pares trenzados de categoría 5e o superior.



2. Conecte el otro extremo del cable a un conector RJ45 del otro dispositivo.

   El indicador de estado del puerto se enciende una vez establecido un vínculo entre el switch y el dispositivo conectado.

   El indicador de estado del puerto se ilumina de color ámbar mientras el protocolo de árbol de expansión (STP) detecta la topología y busca bucles. Esto puede tardar hasta 30 segundos, tras lo cual el indicador de estado del puerto se pone verde.

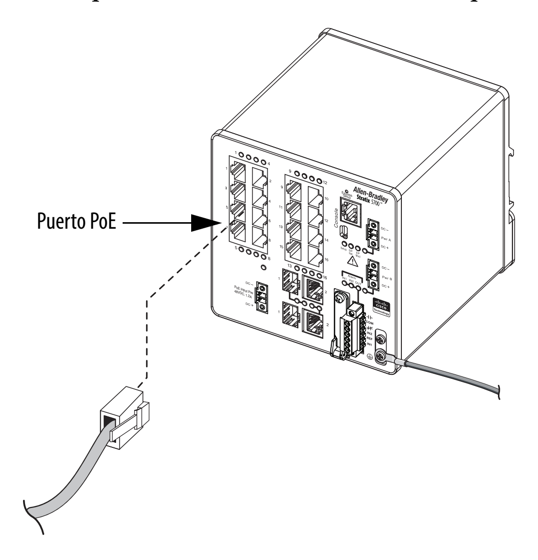
   Las siguientes condiciones pueden impedir que se encienda el indicador de estado del puerto:
   - El dispositivo del otro extremo no está encendido.
   - Existe un problema con un cable o el adaptador instalado en el dispositivo conectado.

3. Reconfigure y reinicie el dispositivo conectado si es necesario.
4. Repita este procedimiento para conectar cada dispositivo.

Conecte puertos PoE

Los switches con puertos PoE necesitan una fuente de alimentación eléctrica independiente. Para determinar los requisitos de la fuente de alimentación eléctrica según la aplicación, consulte la página 37.

1. Inserte un cable Ethernet de tipo directo con cuatro pares trenzados de categoría 5e o superior con un conector RJ45 en el puerto PoE.



2. Inserte el otro extremo del cable a un conector RJ45 del otro dispositivo PoE alimentado.

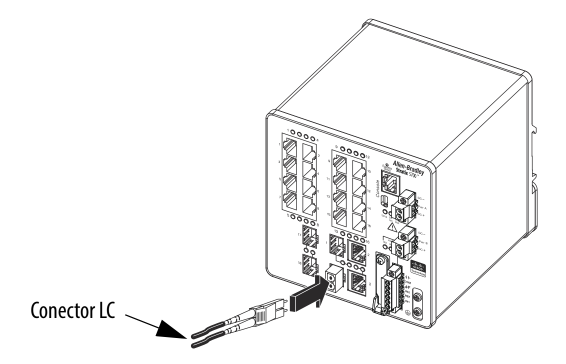
Conecte módulos SFP

Para conectar un cable de fibra óptica a un módulo SFP, siga estos pasos.



ATENCIÓN: No retire los tapones de caucho del puerto del módulo SFP ni las tapas de caucho del cable de fibra óptica hasta que esté listo para conectar el cable. Los tapones y tapas protegen los puertos y cables del módulo SFP frente a la contaminación y la luz ambiental.

1. Retire las cubiertas de caucho del puerto del módulo y del cable de fibra óptica y guárdelos para uso futuro.
2. Inserte un extremo del cable de fibra óptica en el puerto del módulo SFP.



3. Inserte el otro extremo del cable en un receptáculo de fibra óptica del dispositivo objetivo.

4. Observe el indicador de estado del puerto:
   - El indicador de estado se ilumina de color ámbar mientras el módulo SFP detecta la topología de la red y busca bucles. Este proceso tarda unos 30 segundos, tras lo cual el indicador de estado del puerto se pone verde.
   - El indicador de estado se pone verde una vez establecido un vínculo entre el switch y el dispositivo objetivo.
   - El indicador de estado se apaga si el dispositivo objetivo no está encendido o si hay un problema con el cable o el adaptador instalado en el dispositivo objetivo.

   Si es necesario, reconfigure y reinicie el switch o el dispositivo objetivo.

Conecte un puerto de doble uso

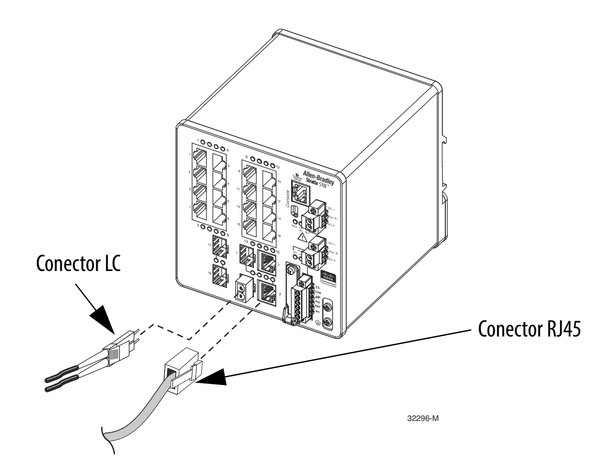
Un puerto de doble función es un solo puerto con dos interfaces: una para un cable RJ45 y otra para un módulo SFP aprobado. Solo puede estar activa una interface a la vez. Si se conectan las dos interfaces, el puerto de módulo SFP tiene prioridad.



ATENCIÓN: No retire los tapones de caucho del puerto del módulo SFP ni las tapas de caucho del cable de fibra óptica hasta que esté listo para conectar el cable. Los tapones y tapas protegen los puertos y cables del módulo SFP frente a la contaminación y la luz ambiental.

Para conectar un puerto de doble función, siga estos pasos.

1. Conecte un conector RJ45 al puerto 10/100/1000 o instale un módulo SFP en la ranura para módulos SFP, y conecte un cable al puerto del módulo SFP.



2. Conecte el otro extremo del cable al otro dispositivo.

   De manera predeterminada, el switch detecta si hay un conector RJ45 o un módulo SFP conectado a un puerto de doble función y configura el puerto según corresponda. Puede cambiar este ajuste y configurar el puerto para reconocer solo un conector RJ45 o solo un módulo SFP mediante el comando de configuración de la interface de tipo de medio físico. Para obtener más información, consulte la documentación correspondiente en http://www.Cisco.com.

Configure inicialmente el switch con Express Setup

Cuando configure el switch por primera vez, use Express Setup para introducir la dirección IP inicial. Al hacer esto se habilita el switch que se va a usar como switch administrado. A continuación podrá obtener acceso al switch a través de la dirección IP para modificar la configuración.

IMPORTANTE	No ejecute Express Setup con una tarjeta SD insertada en el switch.

Necesita este equipo para configurar el switch:

- Una computadora personal con sistema operativo Windows 2000, Windows XP, Windows 2003 o Windows Vista instalado
- Un navegador web compatible (Internet Explorer 9.0, 10.0 y 11.0, o Firefox 25, 26) con JavaScript habilitado
- Un cable de tipo directo o un cable cruzado de categoría 5 para conectar la computadora personal al switch

Haga lo siguiente para configurar la computadora:

- Inhabilite todas las interfaces inalámbricas que se encuentren en ejecución en la computadora personal.
- Inhabilite otras redes de su sistema.
- Establezca la computadora para que determine automáticamente su dirección IP (DHCP) en vez de usar una configuración estática.
- Inhabilite los servidores DNS estáticos.
- Inhabilite los ajustes de proxy del navegador.

Normalmente, los ajustes del navegador están en Tools > Internet Options > Connections > LAN Settings.

Para ejecutar Express Setup, siga estos pasos.

1. Asegúrese de que hay un puerto Ethernet del switch como mínimo disponible para Express Setup.

IMPORTANTE	No use el puerto de la consola para Express Setup.

   Mientras se ejecuta Express Setup, el switch funciona como servidor DHCP. Si la computadora personal tiene una dirección IP estática, cambie la configuración de la computadora personal antes de empezar a usar temporalmente DHCP.

2. Aplique alimentación al switch.

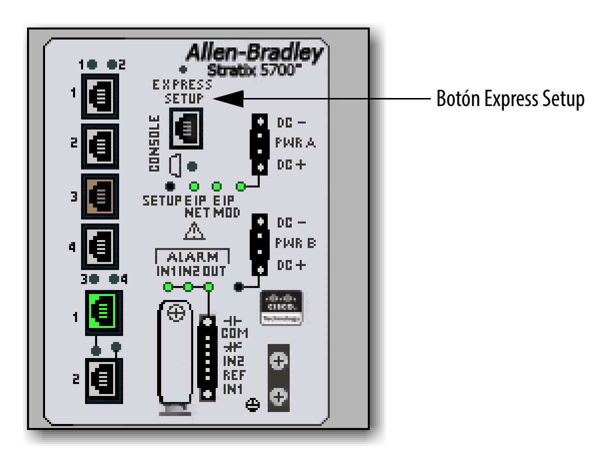
   Una vez aplicada la alimentación al switch, se iniciará su secuencia de encendido. La secuencia de encendido tarda unos 60 segundos en finalizar.

3. Para asegurarse de que la secuencia de encendido ha finalizado, verifique que los indicadores de estado EIP Mod y Setup estén parpadeando de color verde.

   Si falla la secuencia de encendido del switch, el indicador de estado EIP Mod se enciende de color rojo.

4. Presione y suelte el botón Express Setup. Espere unos segundos hasta que el indicador de estado de uno de los puertos del switch no conectados parpadee de color verde.

   Este botón se encuentra ubicado a 16 mm (0.63 pulg.) detrás del panel frontal. Use una herramienta pequeña, como un clip para papeles, para llegar hasta el botón.



5. Conecte un cable Ethernet de categoría 5 (no incluido) entre el puerto parpadeante del switch y el puerto Ethernet de la computadora personal.

   SUGERENCIA Si tarda demasiado en conectar el cable, se apagará el indicador de estado Setup.

   Los dos indicadores de estado de los puertos de la computadora personal y del switch parpadean mientras el switch configura la conexión.

6. Mientras el indicador de estado Setup parpadea de color verde, inicie una sesión en el navegador de Internet en la computadora personal y navegue hasta http://169.254.0.1.

   Si tiene una página de inicio configurada, se cargará la configuración del switch en lugar de su página de inicio normal.

   El switch le pedirá que indique el nombre de usuario y la contraseña predeterminados del switch.

7. Introduzca la contraseña predeterminada del switch: **switch**.

   El nombre de usuario predeterminado es **admin**.

   IMPORTANTE En algunos escenarios, el switch requiere que se introduzca su contraseña varias veces antes de aceptarla.

8. Si no se abre la ventana de Express Setup, haga lo siguiente:
   - Introduzca la URL de un sitio web muy conocido en el navegador para asegurarse de que dicho navegador esté funcionando correctamente. El navegador se dirigirá automáticamente a la página web de Express Setup.
   - Verifique que los ajustes de proxy o los bloqueadores de elementos emergentes estén inhabilitados en el navegador.
   - Verifique que las interfaces inalámbricas estén inhabilitadas en la computadora personal.

9. Rellene los campos.

   Para ver los campos del protocolo industrial común (CIP), debe hacer clic en Advanced Settings.

Network Settings
Host Name:
Management Interface (VLAN): 1
IP Assignment Mode: Static DHCP
IP Address: / 255.255.255.0
Default Gateway:
NTP Server:
User: admin Password: Confirm Password:
Advanced Settings
CIP VLAN: 1
IP Address: /
Same As Management VLAN:
Telnet, CIP and Enable Password: (leave it blank if no change) Confirm Password:
Same As Admin Password
Submit

Campo	Descripción
	Network Settings
Host Name	El nombre del dispositivo.
Management Interface (VLAN ID)	El nombre e ID de la VLAN de administración a través de la que se está administrando el switch. Elija una VLAN existente para que sea la VLAN de administración. La ID predeterminada es 1. El nombre predeterminado de la VLAN de administración es default. El número puede estar entre 1 y 1001. Asegúrese de que el switch y la estación de administración de red estén en la misma VLAN. De otra manera perderá la conectividad de administración con el switch. La VLAN de administración es el dominio de difusión a través del cual se envía el tráfico de administración entre determinados usuarios o dispositivos. Proporciona seguridad y control de difusión para el tráfico de administración que debe limitarse a un determinado grupo de usuarios como, por ejemplo, los administradores de su red. También proporciona acceso administrativo seguro a todos los dispositivos de la red en todo momento.
IP Assignment Mode	El modo de asignación de IP determina si la información de IP del switch se asigna manualmente (estática) o se asigna automáticamente mediante un servidor de protocolo de configuración dinámica de anfitrión (DHCP). El valor predeterminado es Static. Le recomendamos que haga clic en Static y asigne manualmente la dirección IP del switch. En lo sucesivo, podrá utilizar la misma dirección IP siempre que quiera obtener acceso a la interface web del administrador de dispositivos. Si hace clic en DHCP, el servidor DHCP asigna automáticamente una dirección IP, una máscara de subred y un gateway predeterminado al switch. Siempre que el switch no se reinicie, seguirá utilizando la información de IP asignada y usted podrá utilizar la misma dirección IP para obtener acceso a la interface web del administrador de dispositivos. Si asigna manualmente una dirección IP al switch y su red utiliza un servidor DHCP, asegúrese de que la dirección IP que especifique para el switch no esté dentro del rango de direcciones que el servidor DHCP asigna automáticamente a otros dispositivos. Así evitará conflictos de direcciones IP entre el switch y los demás dispositivos.
IP Address	La dirección IP y la máscara de subred asociada son identificadores únicos de un switch en una red: • El formato de dirección IP consiste en una dirección numérica de 32 bits escrita como cuatro números separados por puntos. Cada número puede estar entre 0 y 255. • La máscara de subred es la dirección de red que identifica la subred a la que pertenece el switch. Las subredes sirven para distribuir los dispositivos de una red en grupos más pequeños. La máscara predeterminada es 255.255.255.0. Este campo solo está habilitado si IP Assignment Mode está en Static. Asegúrese de que la dirección IP que asigne al switch no esté utilizada por ningún otro dispositivo de la red. La dirección IP y el gateway predeterminado no pueden ser iguales.

Campo	Descripción
Default Gateway (opcional)	La dirección IP del gateway predeterminado. Un gateway es un encaminador o un dispositivo de red dedicado que permite que el switch se comunique con dispositivos de otras redes o subredes. La dirección IP del gateway predeterminado debe formar parte de la misma subred que la dirección IP del switch. La dirección IP del switch y la dirección IP del gateway predeterminado no pueden ser iguales. Si todos sus dispositivos se encuentran en la misma red y no se utiliza un gateway predeterminado, no es necesario que especifique ninguna dirección IP en este campo. Este campo solo está habilitado si el modo de asignación de IP es Static. Debe especificar un gateway predeterminado si su estación de administración de red y el switch se encuentran en redes o subredes diferentes. De otra manera, el switch y la estación de administración de red no podrán comunicarse entre sí.
NTP Server	La dirección IP del servidor de protocolo de tiempo de red (NTP). El NTP es un protocolo de conexión en red para la sincronización de relojes entre sistemas de computadoras mediante redes de datos de conmutación de paquetes de latencia variable.
User	Escriba el nombre de usuario.
Password, Confirm Password	La contraseña del switch puede tener hasta 63 caracteres alfanuméricos y puede empezar por un número; distingue entre mayúsculas y minúsculas, y puede incluir espacios. La contraseña no puede ser un solo dígito, incluir un símbolo ? o un tabulador, ni espacios al principio o al final. La contraseña predeterminada es **switch**. Para realizar la configuración inicial, debe cambiar la contraseña predeterminada **switch** por otra distinta. Esta contraseña se usa también como contraseña de seguridad del protocolo industrial común (CIP). Le recomendamos que proporcione una contraseña para el switch a fin de proteger el acceso al administrador de dispositivos.
Advanced Settings	
CIP VLAN	La VLAN en la que está habilitado el protocolo industrial común (CIP). La VLAN de CIP debe ser la misma que la VLAN de administración o se puede aislar el tráfico de CIP en otra VLAN que ya se haya configurado en este dispositivo.
IP Address	La dirección IP y máscara de subred de la VLAN de CIP si la VLAN de CIP es diferente a la VLAN de administración. El formato consiste en una dirección numérica de 32 bits escrita como cuatro números separados por puntos. Cada número puede estar entre 0 y 255. Asegúrese de que la dirección IP que asigne a este dispositivo no se utilice para ningún otro dispositivo de la red.
Same As Management VLAN	Indica si los ajustes de la VLAN de CIP son los mismos que los de la VLAN de administración.
Telnet, CIP and Enable Password (opcional), Confirm Password	La contraseña utilizada para la seguridad CIP y Telnet.
Same As Admin Password	Establece la contraseña usada para la seguridad CIP y Telnet para que sea igual a la contraseña de usuario especificada en Network Settings.

10. Haga clic en Submit.

    El switch inicializa su configuración para aplicaciones EtherNet/IP industriales típicas. Seguidamente, el switch lo redirigirá a la página de inicio de sesión de la interface web del administrador de dispositivos. Puede seguir iniciando la interface web del administrador de dispositivos para continuar con la configuración o salir de la aplicación.

11. Desconecte la alimentación de CC en la fuente, desconecte todos los cables del switch e instale el switch en la red.

12. Una vez finalizada la sesión con Express Setup, actualice la dirección IP de la computadora personal:
    - Si se trata de una dirección IP asignada dinámicamente, desconecte la computadora personal del switch y reconéctela a la red. El servidor DHCP de la red asigna una nueva dirección IP a la computadora personal.
    - Si se trata de una dirección IP asignada estáticamente, cámbiela a la dirección IP configurada anteriormente.

Notas:

Características del software del switch

Numeración de puertos

La ID de puerto consta del tipo de puerto (Gigabit Ethernet para puertos Gigabit y Fast Ethernet para puertos de 10/100 Mbps), el número de unidad (siempre 1) y el número de puerto (1-2 para puertos Gigabit o 1-18 para el resto de los puertos, según los números de catálogo). Gigabit Ethernet se abrevia como Gi y Fast Ethernet como Fa.

En la tabla siguiente se muestra la numeración de puertos del switch.

Tabla 2 - Numeración de puertos

N.° de cat.	Descripción	Numeración de los puertos de los rótulos del switch	Numeración de los puertos en el archivo config.text
1783-BMS06SL	Switch administrado de 6 puertos (4 puertos Ethernet; 2 ranuras SFP); firmware Lite	1 2 3 4 5 6	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6
1783-BMS06SA	Switch administrado de 6 puertos (4 puertos Ethernet; 2 ranuras SFP); firmware completo	1 2 3 4 5 6	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6
1783-BMS06TL	Switch administrado de 6 puertos (6 puertos Ethernet); firmware Lite	1 2 3 4 5 6	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6
1783-BMS06TA	Switch administrado de 6 puertos (6 puertos Ethernet); firmware completo	1 2 3 4 5 6	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6
1783-BMS06SGL	Switch administrado de 6 puertos (4 puertos Ethernet; 2 ranuras SFP Gigabit); firmware Lite	1 2 3 4 1 2	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Gi1/1 Gi1/2
1783-BM06SGA	Switch administrado de 6 puertos (4 puertos Ethernet; 2 ranuras SFP Gigabit); firmware completo	1 2 3 4 1 2	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Gi1/1 Gi1/2
1783-BMS06TGL	Switch administrado de 6 puertos (4 puertos Ethernet; 2 puertos Gigabit); firmware completo	1 2 3 4 1 2	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Gi1/1 Gi1/2
1783-BMS06TGA	Switch administrado de 6 puertos (4 puertos Ethernet; 2 puertos Gigabit); firmware completo	1 2 3 4 1 2	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Gi1/1 Gi1/2

Tabla 2 - Numeración de puertos (continuación)

N.° de cat.	Descripción	Numeración de los puertos de los rótulos del switch	Numeración de los puertos en el archivo config.text
1783-BMS10CL	Switch administrado de 10 puertos (8 puertos Ethernet; 2 puertos combinados); firmware Lite	1 2 3 4 5 6 7 8 9 10	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6 Fa1/7 Fa1/8 Fa1/9 Fa1/10
1783-BMS10CA	Switch administrado de 10 puertos (8 puertos Ethernet; 2 puertos combinados); firmware completo	1 2 3 4 5 6 7 8 9 10	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6 Fa1/7 Fa1/8 Fa1/9 Fa1/10
1783-BMS10CGL	Switch administrado de 10 puertos (8 puertos Ethernet; 2	1 2 3 4 5 6 7 8 1 2	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6 Fa1/7 Fa1/8 Gi1/1 Gi1/2
1783-BMS10CGA	Switch administrado de 10 puertos (8 puertos Ethernet; 2 puertos Gigabit combinados); firmware completo	1 2 3 4 5 6 7 8 1 2	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6 Fa1/7 Fa1/8 Gi1/1 Gi1/2
1783-BMS10CGN	Switch administrado de 10 puertos (8 puertos Ethernet; 2 puertos Gigabit combinados); firmware completo; NAT	1 2 3 4 5 6 7 8 1 2	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6 Fa1/7 Fa1/8 Gi1/1 Gi1/2

Tabla 2 - Numeración de puertos (continuación)

N.° de cat.	Descripción	Numeración de los puertos de los rótulos del switch	Numeración de los puertos en el archivo config.text
1783-BMS10CGP	Switch administrado de 10 puertos (8 puertos Ethernet; 2 puertos Gigabit combinados); firmware completo; PTP	1 2 3 4 5 6 7 8 1 2	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6 Fa1/7 Fa1/8 Gi1/1 Gi1/2
1783-BMS12T4E2CGNK	Switch administrado de 18 puertos (12 puertos Ethernet; 4 puertos PoE/PoE+; 2 puertos Gigabit combinados); firmware completo; NAT; revestimiento de conformación	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 1 2	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6 Fa1/7 Fa1/8 Fa1/9 Fa1/10 Fa1/11 Fa1/12 Fa1/13 Fa1/14 Fa1/15 Fa1/16 Gi1/1 Gi1/2
1783-BMS12T4E2CGP	Switch administrado de 18 puertos (12 puertos Ethernet; 4 puertos PoE/PoE+; 2 puertos Gigabit combinados); firmware completo	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 1 2	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6 Fa1/7 Fa1/8 Fa1/9 Fa1/10 Fa1/11 Fa1/12 Fa1/13 Fa1/14 Fa1/15 Fa1/16 Gi1/1 Gi1/2

Tabla 2 - Numeración de puertos (continuación)

N.° de cat.	Descripción	Numeración de los puertos de los rótulos del switch	Numeración de los puertos en el archivo config.text
1783-BMS12T4E2CGL	Switch administrado de 18 puertos (12 puertos Ethernet; 4 puertos PoE/PoE+; 2 puertos Gigabit combinados); firmware Lite	1	Fa1/1
		2	Fa1/2
		3	Fa1/3
		4	Fa1/4
		5	Fa1/5
		6	Fa1/6
		7	Fa1/7
		8	Fa1/8
		9	Fa1/9
		10	Fa1/10
		11	Fa1/11
		12	Fa1/12
		13	Fa1/13
		14	Fa1/14
		15	Fa1/15
		16	Fa1/16
		1	Gi1/1
		2	Gi1/2
1783-BMS20CL	Switch administrado de 20 puertos (16 puertos Ethernet; 2 ranuras SFP; 2 puertos combinados); firmware Lite	1	Fa1/1
		2	Fa1/2
		3	Fa1/3
		4	Fa1/4
		5	Fa1/5
		6	Fa1/6
		7	Fa1/7
		8	Fa1/8
		9	Fa1/9
		10	Fa1/10
		11	Fa1/11
		12	Fa1/12
		13	Fa1/13
		14	Fa1/14
		15	Fa1/15
		16	Fa1/16
		17	Fa1/17
		18	Fa1/18
		19	Fa1/19
		20	Fa1/20
1783-BMS20CA	Switch administrado de 20 puertos (16 puertos Ethernet; 2 ranuras SFP; 2 puertos combinados); firmware completo	1	Fa1/1
		2	Fa1/2
		3	Fa1/3
		4	Fa1/4
		5	Fa1/5
		6	Fa1/6
		7	Fa1/7
		8	Fa1/8
		9	Fa1/9
		10	Fa1/10
		11	Fa1/11
		12	Fa1/12
		13	Fa1/13
		14	Fa1/14
		15	Fa1/15
		16	Fa1/16
		17	Fa1/17
		18	Fa1/18
		19	Fa1/19
		20	Fa1/20

Tabla 2 - Numeración de puertos (continuación)

N.° de cat.	Descripción	Numeración de los puertos de los rótulos del switch	Numeración de los puertos en el archivo config.text
1783-BMS20CGL	Switch administrado de 20 puertos (16 puertos Ethernet; 2 ranuras SFP; 2 puertos Gigabit combinados); firmware Lite	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 1 2	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6 Fa1/7 Fa1/8 Fa1/9 Fa1/10 Fa1/11 Fa1/12 Fa1/13 Fa1/14 Fa1/15 Fa1/16 Fa1/17 Fa1/18 Gi1/1 Gi1/2
1783-BMS20CGN	Switch administrado de 20 puertos (16 puertos Ethernet; 2 ranuras SFP; 2 puertos Gigabit combinados); firmware completo; NAT	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 1 2	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6 Fa1/7 Fa1/8 Fa1/9 Fa1/10 Fa1/11 Fa1/12 Fa1/13 Fa1/14 Fa1/15 Fa1/16 Fa1/17 Fa1/18 Gi1/1 Gi1/2
1783-BMS20CGP	Switch administrado de 20 puertos (16 puertos Ethernet; 2 ranuras SFP; 2 puertos Gigabit combinados); firmware completo; PTP	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 1 2	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6 Fa1/7 Fa1/8 Fa1/9 Fa1/10 Fa1/11 Fa1/12 Fa1/13 Fa1/14 Fa1/15 Fa1/16 Fa1/17 Fa1/18 Gi1/1 Gi1/2

Tabla 2 - Numeración de puertos (continuación)

N.° de cat.	Descripción	Numeración de los puertos de los rótulos del switch	Numeración de los puertos en el archivo config.text
1783-BMS20CGPK	Switch administrado de 20 puertos (16 puertos Ethernet; 2 ranuras SFP; 2 puertos Gigabit combinados); firmware completo; PTP; revestimiento de conformación	1	Fa1/1
		2	Fa1/2
		3	Fa1/3
		4	Fa1/4
		5	Fa1/5
		6	Fa1/6
		7	Fa1/7
		8	Fa1/8
		9	Fa1/9
		10	Fa1/10
		11	Fa1/11
		12	Fa1/12
		13	Fa1/13
		14	Fa1/14
		15	Fa1/15
		16	Fa1/16
		17	Fa1/17
		18	Fa1/18
		1	Gi1/1
		2	Gi1/2

Macro global

Cuando haya finalizado el Express Setup, como se describe en la página 50, el switch ejecutará una macro global (ab-global). Esta macro configura el switch para aplicaciones de automatización industrial típicas que utilizan el protocolo EtherNet/IP. Esta macro configura muchos parámetros, incluidos estos ajustes principales:

- Habilitación de IGMP Snooping y creador de consultas
- Habilitación de CIP
- Configuración de ajustes de QoS y clasificación de CIP, PTP y otro tráfico (no se aplica a switches con revisiones de firmware Lite)
- Habilitación de alarmas, y notificaciones SYSLOG y SNMP
- Habilitación del protocolo de árbol de expansión rápido (RSTP), BPDU Guard, BPDU Filtering y Loop Guard

Si no ejecuta Express Setup para inicializar el switch, no se ejecutará la macro global. Puede usar la CLU para ejecutar la macro global.

Smartports

Smartports son configuraciones recomendadas para los puertos del switch. Estas configuraciones, que se denominan roles de puerto, optimizan las conexiones del switch y proporcionan seguridad, transmisiones de calidad y fiabilidad en el tráfico de los puertos del switch. Los roles de puerto también ayudan a evitar errores de configuración de los puertos.

SUGERENCIA Use roles Smartport inmediatamente después de la configuración inicial del switch para configurar correctamente los puertos del switch antes de conectarlos a los dispositivos.

Optimice los puertos mediante roles de puertos Smartport

Los roles de puertos descritos en la Tabla 3 se basan en el tipo de dispositivos que se van a conectar a los puertos del switch. Por ejemplo, el rol de puerto Desktop for Automation está destinado específicamente a los puertos del switch que se van a conectar a computadoras de escritorio y portátiles.

Personalización de roles Smartport

Los switches Stratix 5700 le permiten crear y modificar hasta 10 roles Smartport personalizados para varias aplicaciones personalizadas. Puede importar o exportar roles Smartport personalizados solo si usa el navegador web Mozilla Firefox, versión 3.6 o superior. De manera predeterminada, los puertos del switch están establecidos en el rol de puerto None.

Tabla 3 - Roles Smartport

Rol de puerto	Descripción
Automation Device	Aplique este rol a los puertos que se van a conectar a dispositivos EtherNet/IP (protocolo industrial Ethernet). Se puede usar para dispositivos de automatización industrial, como controladores lógicos y E/S: • El puerto está establecido en el modo Access. • La seguridad del puerto solo admite una ID MAC. • Optimiza la administración de colas para el tráfico CIP.
Multiport Automation Device	Aplique este rol a los puertos conectados a dispositivos EtherNet/IP multipuertos como, por ejemplo, dispositivos EtherNet/IP con varios puertos distribuidos en una topología lineal o conectada en cadena, el módulo 1783-ETAP (para conexión únicamente al puerto del dispositivo), switches no administrados (como el Stratix 2000™) y switches administrados con el protocolo de árbol de expansión remoto (RSTP) inhabilitado: • El puerto está establecido en el modo Access. • Sin seguridad de puerto. • Administración de colas optimizada para el tráfico CIP.
Desktop for Automation	Aplique este rol a los puertos que se van a conectar a dispositivos de escritorio como, por ejemplo, computadoras de escritorio, estaciones de trabajo, computadoras portátiles y otros anfitriones basados en clientes: • El puerto está establecido en el modo Access. • Portfast habilitado. • La seguridad del puerto solo admite una ID MAC. No lo aplique a los puertos que se van a conectar a switches, encaminadores o puntos de acceso.
Virtual Desktop for Automation	Aplique este rol a los puertos conectados a computadoras que ejecuten software de virtualización. Se puede usar con dispositivos que ejecuten dos direcciones MAC como máximo: • El puerto está establecido en el modo Access. • Portfast está habilitado. • La seguridad del puerto admite dos ID MAC. **IMPORTANTE:** No aplique el rol Virtual Desktop for Automation a puertos conectados a switches, encaminadores o puntos de acceso.
Switch for Automation	Aplique este rol a los puertos que se van a conectar a otros switches con protocolo de árbol de expansión habilitado. El puerto está establecido en el modo Trunk.
Router for Automation	Aplique este rol a los puertos que se van a conectar a encaminadores o switches de capa 3 con servicios de encaminamiento habilitados.

Tabla 3 - Roles Smartport (continuación)

Rol de puerto	Descripción
Phone for Automation	Aplique este rol a los puertos que se van a conectar a teléfonos IP. Se puede conectar al teléfono IP un dispositivo de escritorio como, por ejemplo, una computadora. Tanto el teléfono IP como la computadora conectada tienen acceso a la red a través del puerto: • El puerto está establecido en el modo Trunk. • La seguridad del puerto admite tres ID MAC para este puerto. Este rol da prioridad al tráfico de voz sobre el tráfico general de datos para proporcionar una recepción clara de la voz en los teléfonos IP.
Wireless for Automation	Aplique este rol a los puertos que se van a conectar a puntos de acceso inalámbricos. El punto de acceso puede proporcionar acceso a la red a 30 usuarios inalámbricos como máximo.
Port Mirroring	Aplique este rol a los puertos que se van a monitorear mediante un analizador de red. Para obtener más información acerca de puertos espejo, consulte Puerto espejo en la página 91.
None	Aplique este rol a los puertos si no desea tener un rol Smartport especializado en el puerto. Este rol se puede usar en las conexiones con cualquier dispositivo, incluidos dispositivos en los roles antes descritos.
CS1…CS10	Roles Smartport personalizados. Puede crear un rol de puerto personalizado con un nombre definido por el usuario. Consulte Capítulo 4, Administración del switch mediante la interface web del administrador de dispositivos, para obtener más información sobre la creación de roles Smartport personalizados.

Evite desigualdades de Smartport

Se produce una desigualdad de Smartport cuando un dispositivo conectado no se adapta al rol Smartport aplicado al puerto del switch. Las desigualdades pueden afectar negativamente los dispositivos y a la red.

Las desigualdades pueden ocasionar las siguientes condiciones:

- Alterar el comportamiento del dispositivo conectado
- Disminuir el rendimiento de la red (reducir el nivel de calidad del servicio [QoS]) en el tráfico CIP, de voz, inalámbrico, del switch y del encaminador
- Reducir las restricciones sobre el acceso de invitados a la red
- Reducir la protección frente a ataques de denegación del servicio (DoS) en la red
- Inhabilitar o desactivar el puerto

Se recomienda verificar siempre qué rol Smartport se ha aplicado a un puerto antes de conectar un dispositivo al puerto o de reconectar dispositivos.

Alimentación a través de Ethernet (PoE)

Los switches con puertos PoE son configurables por software y ofrecen las siguientes características:

- Compatibilidad con dispositivos que cumplen con la norma IEEE 802.3af (PoE).
- Compatibilidad con IEEE 802.3at tipo 2 (PoE+), que aumenta la potencia disponible para ser consumida por los dispositivos alimentados de 15.4 a 30 W por puerto.
- Detección automática y provisión de alimentación eléctrica. El switch mantiene una provisión de alimentación eléctrica, monitorea y realiza el seguimiento de las solicitudes de alimentación eléctrica y suministra alimentación solo cuando está disponible.
- Alimentación eléctrica de dispositivos Cisco conectados anteriores a la norma y dispositivos alimentados que cumplen con IEEE 802.3af, si el switch detecta que no hay alimentación eléctrica en el circuito.
- Compatibilidad con el protocolo de detección de Cisco (CDP) con consumo de potencia. Esta característica se aplica solo cuando se usan switches con dispositivos finales Cisco. El dispositivo final Cisco alimentado notifica al switch la cantidad de potencia que está consumiendo. El switch puede suministrar alimentación eléctrica al puerto PoE o interrumpir el suministro.
- Compatibilidad con la administración de alimentación inteligente de Cisco. Un dispositivo final Cisco alimentado y el switch negocian el nivel de consumo de potencia mediante mensajes CDP de negociación de alimentación. La negociación permite que un dispositivo de alta potencia consuma más de 7 W para poder funcionar en su modo de máxima potencia. El dispositivo alimentado arranca primero en el modo de baja potencia, en el que consume menos de 7 W, y entra en negociación para obtener un nivel suficiente de potencia para funcionar en el modo de alta potencia. El dispositivo cambia al modo de alta potencia solo cuando recibe la confirmación del switch.

  La administración de alimentación inteligente de Cisco es compatible con versiones anteriores del CDP con consumo de potencia. El módulo responde de acuerdo con el mensaje del CDP que reciba. El CDP no es compatible con dispositivos alimentados de terceros, por lo que el módulo usa la clasificación IEEE para determinar el consumo de potencia del dispositivo.

Detección de dispositivos alimentados y asignación inicial de alimentación eléctrica

Un switch detecta un dispositivo alimentado cuando hay un puerto activo con capacidad PoE, PoE está habilitado (valor predeterminado) y el dispositivo conectado no está recibiendo alimentación eléctrica de otra fuente de alimentación.

Tras la detección del dispositivo, el switch determina sus requisitos de alimentación eléctrica según del tipo que sea:

- El switch clasifica el dispositivo detectado IEEE compatible con 802.3 af/at dentro de una clase de consumo de potencia. Dependiendo de la provisión de alimentación eléctrica, el switch determina si puede alimentar un puerto PoE. En la tabla siguiente se muestran estos niveles.

Tabla 4 - Clasificaciones de potencia IEEE

Clase	Alimentación eléctrica máxima suministrada por puerto
0 (estado de clase desconocido)	15.4 W
1	4 W
2	7 W
3	15.4 W
4	Solo dispositivos PoE+ de 30 W

- Un dispositivo Cisco alimentado anterior a la norma no proporciona sus requisitos de alimentación eléctrica cuando el switch lo detecta. Un puerto que no se ha configurado para PoE+ asigna 15.4 W inicialmente como provisión de alimentación eléctrica. Un puerto configurado para un switch PoE+ asigna 30 W.

  La asignación inicial de alimentación eléctrica es la cantidad máxima de alimentación eléctrica que necesita un dispositivo alimentado. El switch asigna inicialmente esta cantidad de alimentación eléctrica cuando detecta y alimenta al dispositivo alimentado. Cuando el switch recibe mensajes CDP del dispositivo alimentado y este dispositivo negocia los niveles de alimentación eléctrica con el módulo mediante mensajes CDP de negociación del nivel de alimentación eléctrica, la asignación inicial de alimentación eléctrica puede ser ajustada.

El switch monitorea y realiza un seguimiento de las solicitudes de alimentación eléctrica, y suministra la alimentación eléctrica solo cuando está disponible. El switch realiza un seguimiento de su provisión de alimentación eléctrica, que es la cantidad de alimentación eléctrica disponible en cada puerto PoE. El switch realiza cálculos de alimentación eléctrica cada vez que se proporciona o deniega la alimentación, para mantener actualizada la provisión de alimentación eléctrica.

Después de aplicar alimentación eléctrica a un puerto PoE, el switch usa el CDP (si el dispositivo final Cisco alimentado es compatible con el CDP) para determinar los requisitos reales de consumo de potencia de los dispositivos alimentados conectados y ajusta la provisión de alimentación eléctrica según corresponda. El switch procesa una solicitud y suministra o deniega la alimentación eléctrica. Si se acepta la solicitud, el switch actualiza la provisión de alimentación eléctrica. Si se deniega la solicitud, el switch verifica si se ha

desactivado el suministro de potencia al puerto, genera un mensaje syslog y actualiza los indicadores de estado. Los dispositivos alimentados también pueden negociar un mayor nivel de alimentación eléctrica con el módulo.

Si el switch detecta un fallo causado por una condición de voltaje insuficiente, sobrevoltaje, sobretemperatura, fallo de oscilador o cortocircuito, desactiva el suministro de potencia del puerto, genera un mensaje syslog y actualiza la provisión de alimentación eléctrica y los indicadores de estado.

Modos de administración de alimentación eléctrica

Los puertos PoE admiten estos modos:

- Auto (predeterminado): el puerto detecta automáticamente si el dispositivo conectado necesita alimentación eléctrica. Este es el modo predeterminado. Si el puerto detecta un dispositivo alimentado conectado y el módulo tiene suficiente alimentación eléctrica, la suministra, actualiza la provisión de alimentación eléctrica, activa la alimentación eléctrica del puerto por orden de llegada y actualiza los indicadores de estado.

  Si hay suficiente alimentación eléctrica disponible para todos los dispositivos alimentados conectados al switch, se activa la alimentación eléctrica de todos los dispositivos. Si no hay suficiente alimentación eléctrica disponible para abastecer a todos los dispositivos conectados, y se desconecta y vuelve a conectar un dispositivo mientras otros esperan la llegada de alimentación eléctrica, no se podrá determinar a qué dispositivos se va a suministrar o denegar la alimentación eléctrica.

  Si el suministro de alimentación eléctrica supera la provisión de alimentación eléctrica del sistema, el switch deniega la alimentación eléctrica, verifica si se ha desactivado el suministro de alimentación eléctrica del puerto, genera un mensaje syslog y actualiza los indicadores de estado. Una vez denegada la alimentación eléctrica, el switch vuelve a comprobar la provisión de alimentación eléctrica periódicamente y sigue intentando conceder la solicitud de alimentación eléctrica.

  Si un dispositivo alimentado por el switch se conecta después a una toma de pared, el switch podrá seguir alimentando al dispositivo. El switch podrá seguir informando que sigue suministrando alimentación eléctrica al dispositivo si este recibe alimentación eléctrica del switch o de una fuente de alimentación de CA.

  Si se retira un dispositivo alimentado, el switch detecta automáticamente la desconexión y deja de suministrar alimentación eléctrica al puerto. Puede conectar un dispositivo no alimentado sin dañarlo.

  Puede especificar la potencia máxima permitida para el puerto. Si la potencia máxima de la clase IEEE del dispositivo alimentado es mayor que el valor máximo configurado, el switch no suministra alimentación eléctrica al puerto. Si el switch suministra alimentación eléctrica a un dispositivo final Cisco alimentado, pero el dispositivo alimentado solicita posteriormente mediante mensajes CDP un valor superior al valor máximo configurado, el switch retira la alimentación eléctrica del puerto. La alimentación eléctrica asignada al dispositivo alimentado se reclama como parte de la provisión de alimentación eléctrica global. Si no especifica una potencia, el switch suministra el valor máximo.

- Static: el switch preasigna la alimentación eléctrica al puerto, incluso si no hay ningún dispositivo alimentado conectado, y garantiza que haya alimentación eléctrica disponible para el puerto. El switch asigna la potencia máxima configurada para el puerto, y nunca se ajusta la cantidad mediante la clase IEEE o mediante los mensajes CDP de un dispositivo final Cisco activado. Como la alimentación eléctrica está preasignada, cualquier dispositivo alimentado que use una potencia menor o igual que la máxima tendrá garantizada su alimentación eléctrica cuando se conecte al puerto estático. El puerto dejará de participar en el modelo establecido por el orden de llegada.

  Sin embargo, si la clase IEEE del dispositivo alimentado es mayor que la potencia máxima, el switch no le suministrará alimentación eléctrica. Si el switch recibe mensajes CDP indicando que un dispositivo final Cisco activado necesita una potencia mayor que la máxima, se apagará el dispositivo alimentado.

  Si no especifica una potencia, el switch preasigna el valor máximo. El switch suministra alimentación eléctrica al puerto solo si detecta un dispositivo alimentado. Use el ajuste Static en una interface de alta prioridad.

- Off: el switch inhabilita la detección de dispositivos alimentados y nunca suministra alimentación eléctrica al puerto PoE, aunque se conecte un dispositivo no alimentado. Use este modo solo si desea asegurarse de que no se suministre nunca alimentación eléctrica a un puerto PoE, lo cual lo convierte en un puerto exclusivo para datos.

Asignación máxima de alimentación eléctrica (potencia de corte) en un puerto PoE

El switch determina la potencia de corte de un puerto PoE en este orden:

1. Manualmente, al configurar el nivel de potencia que se va a aprovisionar para el puerto
2. Manualmente, al configurar el nivel de potencia que limita la cantidad de alimentación eléctrica asignada al puerto
3. Automáticamente, cuando el switch establece el consumo de potencia del dispositivo mediante la clasificación IEEE y la negociación de alimentación eléctrica de LLDP o CDP

Si no configura manualmente el valor de la potencia de corte, el switch puede determinar automáticamente el valor mediante la negociación de alimentación eléctrica de CDP cuando esté conectado a un dispositivo final Cisco. Si el switch no puede determinar el valor mediante uno de estos métodos, usará el valor predeterminado de 15.4 W.

Con PoE+, si no configura manualmente el valor de potencia de corte, el switch lo determinará automáticamente mediante la clasificación IEEE del dispositivo, y la negociación de alimentación eléctrica de LLDP o CDP con un dispositivo final Cisco. Si no se ha habilitado CDP o LLDP, se aplica el valor predeterminado de 30 W. Sin embargo, sin CDP o LLDP, el switch no permite que los dispositivos consuman más de 15.4 W porque los valores comprendidos entre 15,400 y 30,000 mW se asignan solo con base en las solicitudes de CDP o LLDP. Si un dispositivo alimentado consume más de 15.4 W sin negociación de CDP o LLDP, es posible que el dispositivo esté infringiendo la limitación de corriente máxima y puede experimentar un fallo al drenar una corriente mayor que el valor

máximo. El puerto se mantiene en el estado de fallo durante un tiempo antes de intentar activarse de nuevo. Si el puerto drena más de 15.4 W de forma continua, el ciclo se repite.

Valores de consumo de potencia

Puede configurar la asignación inicial de alimentación eléctrica y la asignación máxima de alimentación eléctrica de un puerto. Sin embargo, estos valores son solo los valores configurados que determinan cuándo el switch activa o desactiva la alimentación eléctrica del puerto PoE. La asignación máxima de alimentación eléctrica no es igual al consumo real de potencia del dispositivo alimentado. Cuando establece manualmente la asignación máxima de alimentación eléctrica, deberá tener en cuenta la potencia que se pierde por el cable que va desde el puerto al dispositivo alimentado. La potencia de corte es la suma del consumo de potencia nominal del dispositivo alimentado y la pérdida de potencia por el cable en el peor caso.

La cantidad real de potencia consumida por un dispositivo alimentado en un puerto PoE es el valor de potencia de corte más un factor de calibración de 500 mW (0.5 W). El valor de corte real es aproximado y varía con respecto al valor configurado en un porcentaje de dicho valor. Por ejemplo, si la potencia de corte configurada es de 12 W, el valor de corte real es 11.4 W, que es un 0.05% inferior al valor configurado.

Como el switch admite fuentes de alimentación extraíbles externas para PoE/PoE+ y puede configurar la provisión según la fuente de alimentación usada, la cantidad total de potencia disponible para los dispositivos alimentados varía en función de la configuración de la fuente de alimentación:

- Si se elimina una fuente de alimentación y se sustituye por una nueva que suministre menos potencia y el módulo no tiene suficiente potencia para los dispositivos alimentados, el switch deniega la alimentación eléctrica a los puertos PoE que estén en el modo Auto siguiendo los números de puerto en orden descendente. Si el switch sigue sin tener suficiente potencia, denegará la alimentación a los puertos PoE que estén en modo Static siguiendo los números de puerto en orden descendente.

- Si la nueva fuente de alimentación eléctrica suministra más potencia que la anterior y el switch tiene ahora más potencia disponible, el switch suministrará potencia a los puertos PoE que estén en modo Static siguiendo los números de puerto en orden ascendente. Si todavía tiene potencia disponible, el switch suministrará alimentación eléctrica a los puertos PoE que estén en modo Auto siguiendo los números de puerto en orden ascendente.

IMPORTANTE	Para asignar la alimentación eléctrica de manera precisa, se debe configurar manualmente la potencia de la fuente de alimentación eléctrica mediante la interface web del administrador de dispositivos o el CIP.

Redes VLAN

Una red de área local virtual (VLAN) es un segmento lógico de usuarios y recursos de red agrupados por función, equipo o aplicación. Esta segmentación no se realiza teniendo en cuenta la ubicación física de los usuarios y recursos. Por ejemplo, las redes VLAN pueden estar basadas en los departamentos de su empresa o en grupos de usuarios que se comunican principalmente entre ellos.

El switch incluye una VLAN predeterminada a la que inicialmente pertenece cada puerto del switch. El switch admite un máximo de 255 redes VLAN, incluida la VLAN predeterminada.

Cada VLAN se identifica mediante su nombre y número de ID. La VLAN predeterminada se denomina default. La ID puede ser de 1 a 1001 y de 1005 a 4094, donde 1 es la ID predeterminada.

Puede asignar puertos del switch ya sea a la VLAN predeterminada o bien a las VLAN que ha creado. La VLAN predeterminada por sí sola puede ser suficiente dependiendo del tamaño y los requisitos de su red. Le recomendamos que determine primero sus necesidades de redes VLAN antes de crear redes VLAN.

Con Smartports personalizados, puede especificar el tipo de VLAN que desee implementar en ese puerto.

La VLAN predeterminada es también la VLAN de administración. Tras la configuración inicial, puede crear más redes VLAN y designar cualquier VLAN del switch como la VLAN de administración. La VLAN de administración proporciona acceso administrativo al switch. Debe asignar uno de los puertos del switch a la VLAN de administración. De otra manera, no tendrá acceso al switch para fines administrativos. Inicialmente todos los puertos se asignan a la VLAN de administración.

Puede asignar todos los puertos, independientemente de su rol Smartport, a la VLAN predeterminada (default).

Aisle tráfico y usuarios

Con las redes VLAN se pueden aislar diferentes tipos de tráfico, como voz y datos, para conservar la calidad de la transmisión y minimizar el exceso de tráfico entre los segmentos lógicos. Las VLAN se pueden usar también para aislar diferentes tipos de usuarios. Por ejemplo, se pueden limitar las difusiones de datos específicos a determinados grupos de trabajo lógicos por motivos de seguridad como, por ejemplo, para mantener la información sobre los salarios de los empleados solo en los dispositivos de una VLAN creada para comunicaciones relacionadas con la nómina.

Una ventaja adicional del uso de las VLAN es la reducción del esfuerzo administrativo necesario para examinar sistemáticamente las solicitudes de recursos de red.

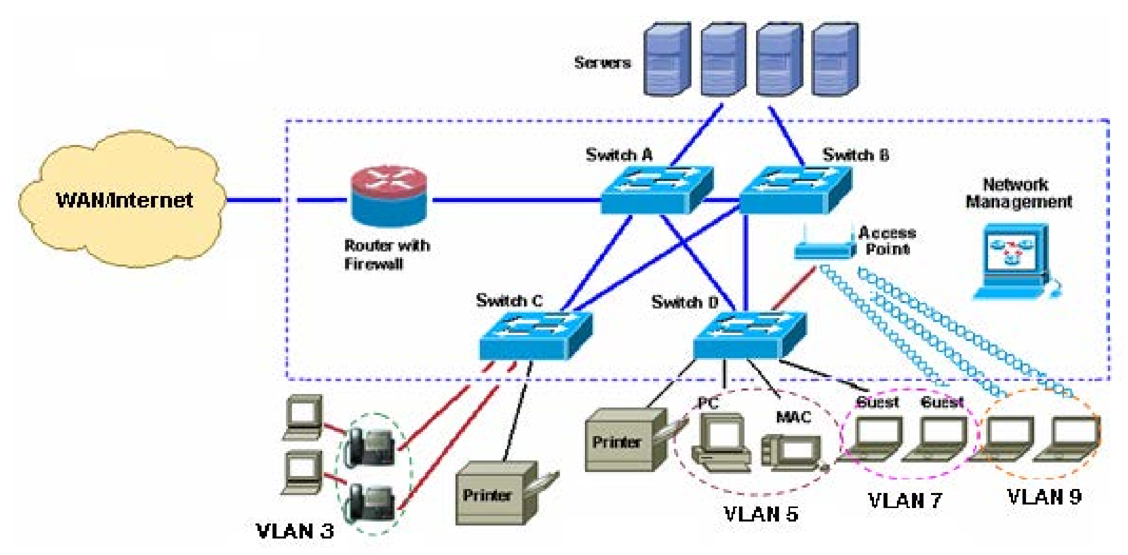
Las VLAN aíslan partes de la red. Por tanto, los dispositivos conectados a los puertos del switch de la misma VLAN (usuarios de red de la misma VLAN) solo pueden comunicarse entre ellos y pueden compartir los mismos datos.

Los dispositivos conectados a los puertos del switch de VLAN diferentes no pueden comunicarse entre sí a través del switch, a menos que este se haya configurado para el encaminamiento. Se debe configurar un switch Stratix 5700, un encaminador o un switch de capa 3 para habilitar el encaminamiento a través de las VLAN (encaminamiento entre VLAN) y, además, se deben establecer políticas de seguridad adicionales.

Si la red también usa un servidor DHCP, asegúrese de que el servidor está accesible para los dispositivos de todas las VLAN.

La figura siguiente presenta un ejemplo de red que utiliza redes VLAN basadas en diferentes tipos de tráfico de red y usuarios de red. La organización de una red en torno a estos factores facilita la definición del tamaño y la afiliación de las VLAN en la red.

Figura 1 - Ejemplo de VLAN



Aisle diferentes tipos de tráfico

El aislamiento del tráfico de datos con respecto al tráfico sensible a los retardos, como el tráfico de voz, mejora la calidad de las transmisiones de voz. En la figura anterior, los puertos del switch conectados a los teléfonos IP pertenecen a la VLAN 3, una VLAN que se ha configurado para proporcionar servicios de voz sobre IP (VoIP) en estas conexiones, lo que significa que se le da prioridad al tráfico de voz sobre el tráfico de datos IP normal. El tráfico de voz del teléfono y las solicitudes de servicio telefónico IP para un servidor de PBX IP tienen prioridad sobre los dispositivos de escritorio conectados a los teléfonos IP.

Para aislar aún más el tráfico de datos del tráfico de voz, el tráfico de datos proveniente de los dispositivos de escritorio conectados se puede asignar a una VLAN independiente.

Agrupe usuarios

La red mostrada en la Figura 1 permite obtener acceso a los tres tipos de usuarios de red:

- Empleados cableados
- Empleados inalámbricos
- Visitantes de la empresa cableados o inalámbricos

Cada tipo de usuario necesita diferentes niveles de acceso a la red de la empresa. Las VLAN y las políticas de seguridad de un encaminador o un switch de capa 3 pueden imponer privilegios y restricciones a diferentes tipos de usuarios.

Consulte la Figura 1 en la página 70:

- La VLAN 5 ofrece un acceso de nivel de empleado a los recursos de la empresa. Este tipo de acceso de red necesita una conexión directa a los puertos específicos del switch.

- La VLAN 7 ofrece acceso solo a Internet a los visitantes de la empresa. Los visitantes con conexiones cableadas o inalámbricas a los puertos del switch se asignan a esta VLAN, que limita automáticamente el acceso de los invitados a Internet únicamente.

- La VLAN 9, que tiene uno más puertos del switch conectados al punto de acceso inalámbrico, impone políticas de seguridad para identificar al usuario inalámbrico (por ejemplo, como empleado o como invitado) y determinar lo que puede hacer el usuario en la red (por ejemplo, obtener acceso solo a Internet u obtener acceso a otros recursos de red).

IGMP Snooping con creador de consultas

Los switches de capa 2 pueden usar IGMP Snooping para impedir el desbordamiento del tráfico de multidifusión mediante la configuración dinámica de interfaces de capa 2, de manera que el tráfico de multidifusión se reenvíe solo a las interfaces asociadas a dispositivos de multidifusión IP. IGMP Snooping exige que el switch de LAN escuche las transmisiones de IGMP entre el anfitrión y el encaminador, y realice un seguimiento de los grupos de multidifusión y los puertos miembros. Cuando el switch recibe un informe de IGMP de un anfitrión para un grupo de multidifusión específico, el switch añade el número de puerto del anfitrión a la entrada de tabla de reenvío; cuando recibe un mensaje IGMP Leave Group de un anfitrión, elimina el puerto anfitrión de la entrada de tabla. También elimina periódicamente las entradas si no recibe informes de afiliación IGMP de los clientes de multidifusión.

El encaminador de multidifusión envía consultas generales periódicas a todas las VLAN. Todos los anfitriones interesados en este tráfico de multidifusión envían solicitudes de incorporación y se añaden a la entrada de la tabla de reenvío. El switch crea una entrada por VLAN en la tabla de reenvío de multidifusión IP de IGMP Snooping para cada grupo desde el que reciba una solicitud de incorporación de IGMP.

El switch admite la conexión en puente basada en grupos de multidifusión IP en lugar de grupos basados en direcciones MAC. Con los grupos basados en direcciones MAC de multidifusión, si una dirección IP que se esté configurando se traduce (mediante alias) en una dirección MAC anteriormente configurada o en cualquier dirección MAC de multidifusión reservada (en el rango de 224.0.0.xxx), el comando fallará. Como el switch usa grupos de multidifusión IP, no hay problemas de uso de alias para direcciones.

256 es el número predeterminado de grupos de multidifusión admitidos en los switches. Si supera los 180 grupos de multidifusión, le recomendamos que cambie a la plantilla SDM de encaminamiento mediante la CLI.

Los grupos de multidifusión IP detectados mediante IGMP Snooping son dinámicos. Si especifica una afiliación de grupo para la dirección de un grupo de multidifusión de manera estática, su ajuste sustituirá a cualquier manejo automático de IGMP Snooping. Las listas de afiliación de grupos de multidifusión pueden incluir tanto ajustes definidos por el usuario como ajustes determinados mediante IGMP Snooping. Las direcciones IP de multidifusión usadas por la red EtherNet/IP para el tráfico de E/S son detectadas por el switch.

La implementación de IGMP en el switch es IGMP V2. Esta versión es compatible con versiones anteriores de switches que ejecuten IGMP -V1. El switch tiene una función de creación de consultas incorporada, y la macro global habilita IGMP Snooping y el creador de consultas.

Protocolo de árbol de expansión

El protocolo de árbol de expansión (STP) es un protocolo de administración de vínculos de capa 2 que proporciona redundancia de ruta a la vez que impide que se produzcan bucles en la red. Para que una red Ethernet de capa 2 funcione correctamente, solo puede existir una ruta activa entre dos estaciones. La existencia de varias rutas activas entre estaciones finales genera bucles en la red. Si hay un bucle en la red, las estaciones finales pueden recibir mensajes duplicados. Los switches también pueden detectar direcciones MAC de estaciones finales en varias interfaces de capa 2. Estas condiciones generan inestabilidad en la red. E funcionamiento de los árboles de expansión es transparente para las estaciones finales, que no pueden detectar si están conectadas a un segmento único de LAN o a una LAN conmutada de varios segmentos.

El STP usa un algoritmo de árbol de expansión para seleccionar un switch de una red conectada de manera redundante como raíz del árbol de expansión. El algoritmo calcula la mejor ruta sin bucles a través de una red de capa 2 conmutada, para lo cual asigna un rol a cada puerto basado en el rol del puerto de la topología activa:

- Root: puerto de reenvío elegido para la topología del árbol de expansión
- Designated: puerto de reenvío elegido para cada segmento de LAN conmutada
- Alternate: puerto bloqueado que proporciona una ruta alternativa al puente raíz del árbol de expansión
- Backup: puerto bloqueado de una configuración de realimentación

El switch que tenga todos sus puertos como el rol designado o como el rol de respaldo es el switch raíz. El switch que tenga uno de sus puertos como mínimo en el rol designado se denomina switch designado.

El árbol de expansión fuerza las rutas de datos redundantes a un estado de reserva (bloqueado). Si un segmento de red del árbol de expansión falla y existe una ruta redundante, el algoritmo de árbol de expansión vuelve a calcular la topología del árbol de expansión y activa la ruta de reserva. Los switches envían y reciben tramas del árbol de expansión, denominadas unidades de datos del protocolo puente (BPDU), a intervalos regulares. Los switches no reenvían estas tramas, pero las usan para construir una ruta sin bucles. Las BPDU contienen información acerca del switch de envío y sus puertos, que incluye el switch y las direcciones MAC, la prioridad del switch, la prioridad de los puertos y el costo de la ruta. El árbol de expansión usa esta información para elegir el switch raíz y el puerto raíz para la red conmutada, y el puerto raíz y el puerto designado para cada segmento conmutado.

Puede elegir una de estas opciones:

- El protocolo de árbol de expansión rápido (RSTP) predeterminado (conocido también como protocolo de árbol de expansión múltiple [MST])
- Protocolo de árbol de expansión por VLAN (PVST+)
- Protocolo de árbol de expansión rápido por VLAN (RPVST+)

SUGERENCIA Si va a conectar el switch a un switch de red Cisco, el valor predeterminado típico es PVST+, no RSTP. Para lograr compatibilidad, se debe modificar uno u otro switch.

Umbrales de puertos

Los umbrales de puertos impiden que el tráfico de una LAN se vea afectado por una tormenta de difusión, multidifusión o unidifusión en una de las interfaces físicas. Los umbrales de puertos no se aplican a switches con firmware Lite.

Una tormenta de LAN se produce cuando los paquetes inundan la LAN, lo que crea un tráfico excesivo y degrada el rendimiento de la red. Los errores en la implementación de la pila de protocolos, los errores en las configuraciones de redes o los usuarios que generan ataques de denegación del servicio pueden provocar una tormenta.

Entrante (control de tormentas)

Los umbrales de puertos de entrada (o supresión de tráfico) monitorean los paquetes que pasan de una interface al bus de conmutación y determinan si el paquete es de unidifusión, multidifusión o difusión. El switch cuenta el número de paquetes de un tipo especificado que se ha recibido en el intervalo de tiempo de un segundo y compara la medición con un umbral de nivel de supresión predefinido.

Los umbrales de puertos usan uno de estos métodos para medir la actividad de tráfico:

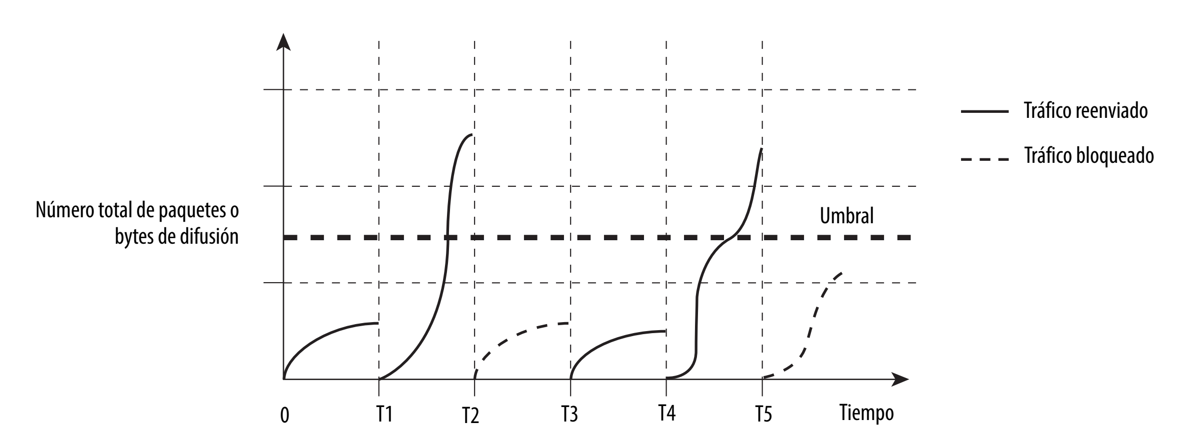
- El ancho de banda como porcentaje del ancho de banda total disponible del puerto que puede usar el tráfico de difusión, multidifusión o unidifusión.
- La velocidad del tráfico, en paquetes por segundo, a la que se reciben los paquetes de difusión, multidifusión o unidifusión.
- La velocidad del tráfico, en bits por segundo, a la que se reciben los paquetes de difusión, multidifusión o unidifusión.

Con cada método, el puerto bloquea el tráfico cuando se alcanza el umbral ascendente. El puerto sigue bloqueado hasta que la velocidad del tráfico cae por debajo del umbral descendente y seguidamente reanuda el reenvío normal.
En general, cuanto más alto es el nivel, menos efectiva será la protección frente a tormentas de difusión.

IMPORTANTE	Cuando se alcanza el umbral del puerto para el tráfico de multidifusión, se bloquea todo el tráfico de multidifusión, excepto el tráfico de administración de redes, como las tramas de las unidades de datos del protocolo puente (BDPU) y el protocolo de detección de Cisco (CDP).

El gráfico muestra los patrones del tráfico de difusión de una interface durante un determinado período de tiempo. El ejemplo también se puede aplicar al tráfico de multidifusión y unidifusión. En este ejemplo, el tráfico de difusión que se reenvía supera el umbral configurado entre los intervalos de tiempo T1 y T2, y entre T4 y T5. Cuando la cantidad de tráfico especificado supera el umbral, se interrumpe todo el tráfico de ese tipo durante el siguiente período de tiempo. Por tanto, el tráfico de difusión se bloquea durante los intervalos posteriores a T2 y T5. En el siguiente intervalo de tiempo (por ejemplo, T3), si el tráfico de difusión no supera el umbral, se vuelve a reenviar.

Figura 2 - Ejemplo de umbrales de puertos



La combinación del nivel de supresión del control de tormentas y el intervalo de tiempo de un segundo controla el funcionamiento del algoritmo de los umbrales de puertos. Un umbral más alto permite transferir más paquetes. Un valor de umbral del 100% significa que no se aplica ningún límite al tráfico. Un valor de 0.0 significa que todo el tráfico de difusión, multidifusión o unidifusión de ese puerto está bloqueado.

IMPORTANTE	Como los paquetes no llegan a intervalos regulares, el intervalo de tiempo de un segundo durante el cual se mide la actividad del tráfico puede afectar al comportamiento de los umbrales de puertos.

Saliente (limitación de velocidad)

Los umbrales de puertos salientes limitan la velocidad a la que se comunica el switch con un dispositivo cliente como porcentaje de la velocidad del cable (magnitud del límite de velocidad como porcentaje del total). La limitación del ancho de banda que se impone a determinados usuarios y puertos ayuda a controlar la congestión de la red, lograr un alto rendimiento, crear redes eficientes e impedir que un número reducido de dispositivos monopolicen el ancho de banda de la red. También puede mejorar la confiabilidad, ya que limita el ancho de banda de los dispositivos finales que no pueden manejar niveles de tráfico muy elevados. Desde la interface web del administrador de dispositivos o el AOP de la aplicación Logix Designer se puede habilitar o inhabilitar la limitación de velocidad a nivel de cada puerto.

Configuración predeterminada de umbrales de puertos

De manera predeterminada, los umbrales de puertos de difusión, multidifusión o unidifusión entrantes están inhabilitados. Los umbrales de puertos salientes también están inhabilitados.

Seguridad de puertos

Los switches Stratix 5700 implementan la seguridad de puertos con base en las direcciones MAC. Una dirección MAC es una dirección única asignada a cada dispositivo compatible con Ethernet. Esto significa que el switch puede imponer comunicaciones, ya sea de manera dinámica o estática, a nivel de cada dirección MAC.

Con una seguridad de puertos dinámica, el puerto de un switch se comunica con un determinado número de dispositivos (direcciones MAC). El puerto realiza un seguimiento solo del número de dispositivos, en lugar de las direcciones MAC de dichos dispositivos. La seguridad de puertos estática añade dispositivos a la tabla de seguridad de puertos a nivel de cada dirección MAC. Con una seguridad de puertos estática/dinámica, solo los dispositivos con las direcciones MAC que aparecen en la tabla de seguridad se pueden comunicar en ese puerto.

Uno o ambos métodos se pueden usar en los switches Stratix 5700 con un firmware completo a nivel de cada puerto. La seguridad de puertos no se aplica a switches con firmware Lite.

Dirección MAC segura dinámica (ID MAC)

Muchos roles Smartport tienen un número máximo de ID MAC que puede usar ese puerto. Por ejemplo, el rol Smartport “Automation Device” configura el puerto para una ID MAC como máximo. La ID MAC es dinámica, lo que significa que el switch detecta la primera ID MAC de origen que va a usar el puerto. Los intentos de acceso al puerto que realice cualquier otra ID MAC serán denegados.

Si el vínculo se torna inactivo, el switch vuelve a detectar de manera dinámica la ID MAC para su protección.

El número predeterminado de ID MAC se puede modificar en la ficha Port Security de la interface web del administrador de dispositivos o la aplicación Logix Designer.

En la tabla siguiente se muestra el rol Smartport y el número máximo de ID MAC admitidas.

Tabla 5 - Número máximo de ID MAC por rol Smartport

Rol Smartport	Número de ID MAC (máx.)
Automation Device	1
Desktop for Automation	1
Switch for Automation	Sin limitaciones
Router for Automation	Sin limitaciones
Phone for Automation	3
Wireless for Automation	Sin limitaciones
Multiport Automation Devices	Sin limitaciones
Virtual Desktop for Automation	2
Port Mirroring	Sin limitaciones
None	Sin limitaciones

Dirección MAC segura estática (ID MAC)

El otro método de limitación de ID MAC consiste en configurar estáticamente una o más ID MAC para un puerto definiéndolas en la ficha Port Security de la interface web del administrador de dispositivos. Estas direcciones pasan a formar parte de la configuración guardada del switch. Este método proporciona un alto grado de protección. Sin embargo, si usted sustituye algún dispositivo conectado al puerto, debe volver a configurar las ID MAC porque los nuevos dispositivos tienen ID MAC diferentes a las de los dispositivos anteriores.

Infracciones de seguridad

Se produce una infracción de seguridad cuando ocurre alguna de estas situaciones:

- Se ha añadido a la tabla de direcciones el número máximo de direcciones MAC seguras que se han configurado para un puerto, y una estación cuya dirección MAC no se encuentra en la tabla de direcciones intenta obtener acceso a la interface.

- Una dirección detectada o configurada en una interface segura aparece en otra interface segura de la misma VLAN.

Cuando se produce una infracción, el puerto pasa al modo Restrict. En este modo, los paquetes con direcciones de origen desconocidas se desechan y usted recibe una notificación de que se ha producido una infracción de seguridad. Se envía una interrupción de SNMP, se registra un mensaje syslog y se incrementa el contador de infracciones.

EtherChannels

Un EtherChannel (o grupo de puertos) es un grupo de dos o más puertos de switch Fast Ethernet o Gigabit Ethernet empaquetados en un único vínculo lógico, lo cual crea un vínculo de ancho de banda superior entre los dos switches.

El switch admite hasta seis EtherChannels. Cada EtherChannel puede incluir hasta ocho puertos Ethernet configurados compatibles. Los EtherChannels no se aplican a switches con firmware Lite.

La figura siguiente muestra dos EtherChannels. Dos puertos full-duplex de 10/100/1000 Mbps en los switches A y C crean un EtherChannel con un ancho de banda de hasta 4 Gbps entre ambos switches. De manera similar, dos puertos full-duplex 10/100 en los switches B y D crean un EtherChannel con un ancho de banda de hasta 400 Mbps entre ambos switches.

Si uno de los puertos del EtherChannel deja de estar disponible, el tráfico se envía a través del resto de los puertos del EtherChannel.

Figura 3 - Ejemplo de EtherChannel

Puede configurar un EtherChannel en uno de estos modos:

- Port Aggregation Protocol (PAgP)
- Link Aggregation Control Protocol (LACP)
- On

Configure ambos extremos del EtherChannel en el mismo modo:

- Cuando configure un extremo de un EtherChannel en el modo PAgP o LACP, el sistema negociará con el otro extremo del canal para determinar los puertos que se vuelven activos. Se suspenden los puertos incompatibles. En lugar de pasar al estado suspendido, el puerto local pasa a un estado independiente y sigue transportando tráfico de datos como cualquier otro vínculo. La configuración del puerto no cambia, pero el puerto no participa en el EtherChannel.

- Cuando configura un EtherChannel en el modo On, no se realiza ninguna negociación. El switch obliga a todos los puertos compatibles a volverse activos en el EtherChannel. El otro extremo del canal (en el otro switch) se debe configurar también en el modo On; de otra manera, se pueden perder paquetes.

Si falla un vínculo dentro de un EtherChannel, el tráfico anteriormente transportado por ese vínculo fallido se desplaza al resto de vínculos del EtherChannel. Si se habilitan interrupciones en el switch, se envía una interrupción en respuesta a un fallo que identifique el switch, el EtherChannel y el vínculo fallido. Los paquetes de difusión y multidifusión que llegan por un vínculo de un EtherChannel se bloquean y no pueden regresar por ningún otro vínculo del EtherChannel.

Persistencia de DHCP

Cada uno de los dispositivos de una red basada en IP debe tener una dirección IP única. El protocolo de configuración dinámica de anfitrión (DHCP) asigna automáticamente la información de direcciones IP de un grupo de direcciones disponibles a dispositivos recién conectados (clientes DHCP) en la red. Si un dispositivo deja la red y posteriormente se vuelve a incorporar a ella, el dispositivo recibe la siguiente dirección IP disponible, que puede ser (o no) la misma que tenía antes.

El switch se puede establecer para funcionar como servidor DHCP y proporcionar persistencia de DHCP. Con la persistencia de DHCP, usted puede asignar una dirección IP específica a cada puerto para asegurarse de que un dispositivo conectado a un puerto determinado reciba la misma dirección IP. Esta característica funciona únicamente con un solo dispositivo conectado a cada puerto configurado para persistencia de DHCP.

IMPORTANTE	Para asegurarse de que la persistencia de DHCP funciona correctamente, siga las normas de aplicación.

Sincronización de hora CIP Sync (protocolo de tiempo de precisión)

El estándar IEEE 1588 define un protocolo denominado protocolo de tiempo de precisión (PTP) que permite sincronizar con precisión los relojes de los sistemas de medición y control. Esto se denomina sincronización de hora CIP Sync. Los relojes se sincronizan por la red de comunicación EtherNet/IP. El PTP permite la sincronización de sistemas que incluyen relojes de diferente precisión, resolución y estabilidad. El PTP genera una relación maestro-esclavo entre los relojes del sistema. Todos los relojes obtienen en última instancia su hora de un reloj seleccionado como reloj Grandmaster.

Hay tres modos de PTP disponibles para los switches:

- Boundary Clock
- Transparent Clock
- Forwarding (el PTP se inhabilita cuando se selecciona el modo Forwarding)

Para obtener más información sobre estos modos, consulte el documento Converged Plantwide Ethernet Design and Implementation Guide, publicación ENET-TD001.

El modo predeterminado de PTP es el modo Forwarding.

Traducción de direcciones de red (NAT)

NAT es un servicio que traduce una dirección IP en otra dirección IP a través de un switch configurado para NAT. El switch traduce las direcciones de origen y destino de los paquetes de datos cuando el tráfico pasa entre las subredes.

Este servicio es útil si necesita volver a utilizar direcciones IP a lo largo de una red. Por ejemplo, NAT permite que los dispositivos que comparten una misma dirección IP en una subred privada se segmenten en varias subredes privadas idénticas mientras mantienen identidades únicas en la subred pública.(1)

La implementación de NAT en el switch Stratix 5700 se distingue de estas maneras:

- NAT uno a uno: el switch usa una NAT uno a uno, en lugar de una NAT uno-a-muchos. Una NAT uno-a-uno requiere que cada dirección de origen se traduzca en una dirección de destino única. A diferencia de la NAT uno-a-muchos, no es posible que varias direcciones de origen compartan una misma dirección de destino.
- Implementación de capa 2: la implementación de la NAT del switch funciona al nivel de capa 2 (MAC). A este nivel, el switch solo puede sustituir direcciones IP y no funciona como encaminador.

Descripción general de la configuración

Para configurar NAT, deben crearse una o más ocurrencias únicas de NAT. En una implementación típica, solo se necesita una ocurrencia. Una ocurrencia de NAT contiene entradas que definen cada traducción de dirección, así como otros parámetros de configuración.

Las traducciones que defina dependerán de si el tráfico se encamina a través de un encaminador o un switch de capa 3, o de un switch de capa 2:

- Si el tráfico se encamina a través de un encaminador o un switch de capa 3 (Figura 4), defina lo siguiente:
  – Una traducción de privada a pública por cada dispositivo de la subred privada que necesite comunicarse en la subred pública.
  – Traducción de un gateway para el encaminador o switch de capa 3.

  No tiene que configurar NAT para todos los dispositivos de la subred privada. Por ejemplo, puede optar por omitir algunos dispositivos de NAT para aumentar la seguridad, disminuir el tráfico o conservar espacio para direcciones públicas.

IMPORTANTE	La mejor práctica que le podemos recomendar es que encamine el tráfico a través de un encaminador o switch de capa 3.

- Si el tráfico se encamina a través de un switch de capa 2 (Figura 5), defina lo siguiente:
  – Una traducción de privada a pública por cada dispositivo de la subred privada que necesite comunicarse en la subred pública.
  – Una traducción de pública a privada por cada dispositivo de la subred pública que necesite comunicarse en la subred privada.

(1) Tenga en cuenta que los términos privado y público se usan para diferenciar las dos redes situadas a cada lado del dispositivo NAT. Esto no implica que la red pública tenga que ser encaminable por Internet.

Figura 4 - Ejemplo de capa 3

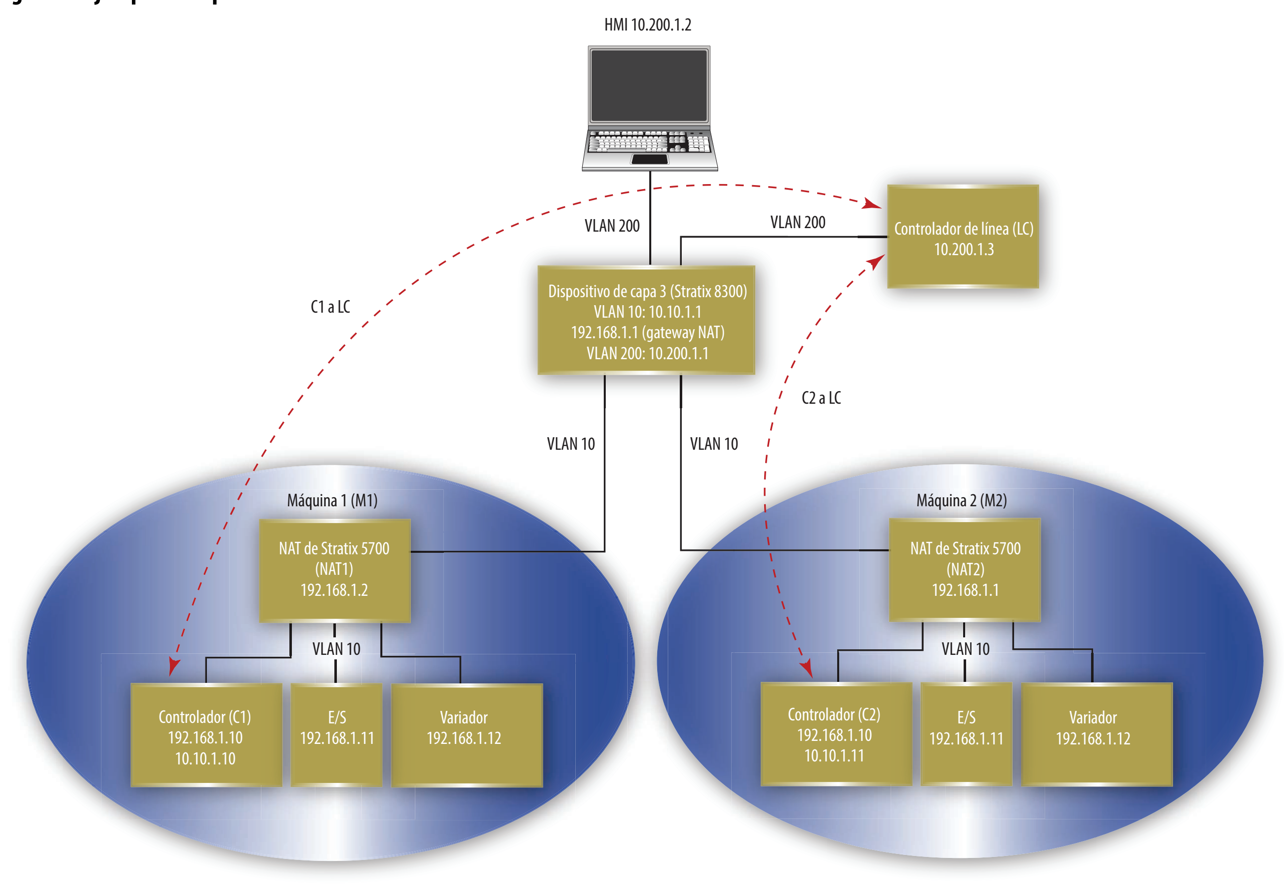
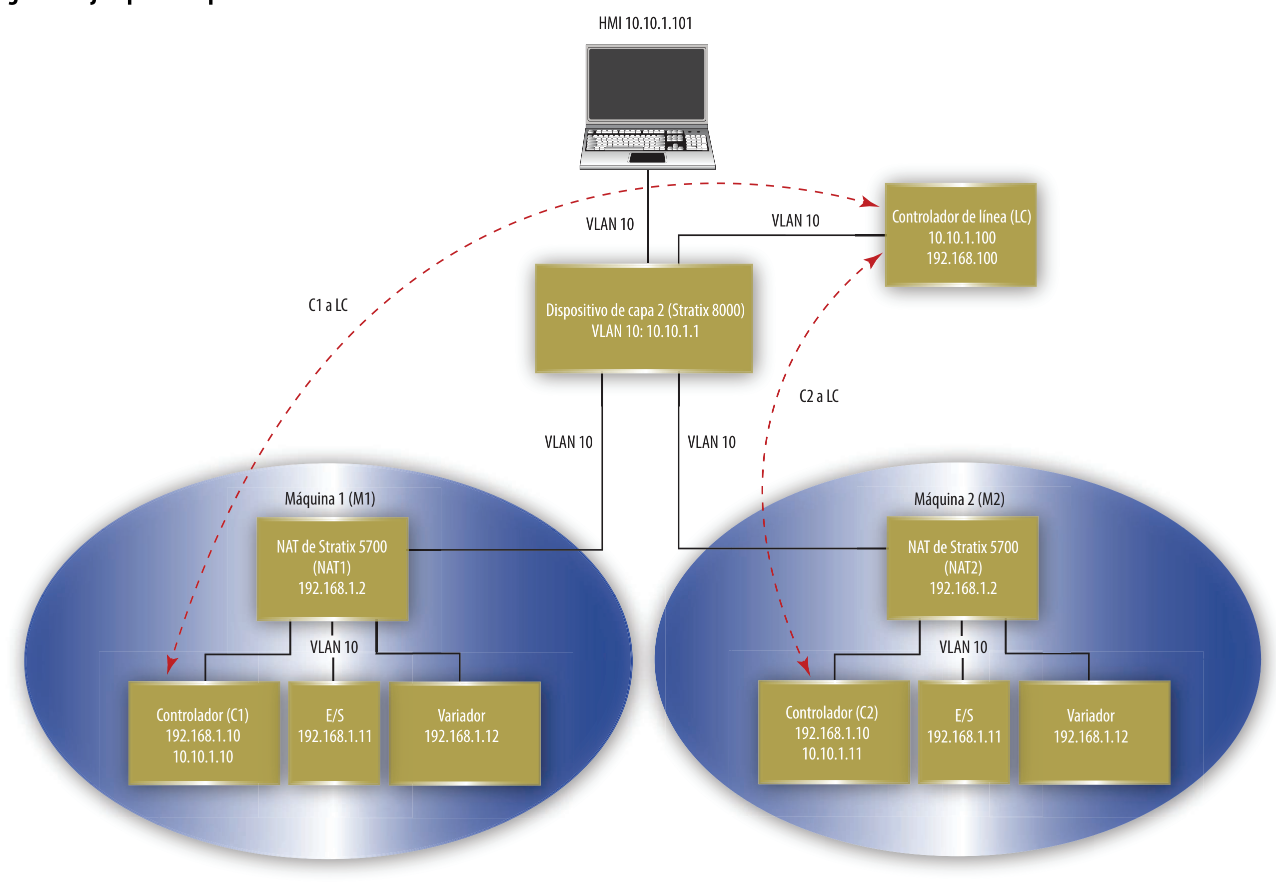


Figura 5 - Ejemplo de capa 2



La traducción de una dirección puede ser de uno de tres tipos. El tipo de traducción determina el número de entradas de traducción. Un switch puede tener 128 entradas de traducción como máximo.

Tabla 6 - Número de entradas de traducción por tipo de traducción

Tipo de traducción	Entradas de traducción	Descripción
Single	1	Traduce una dirección IP única. Consta de lo siguiente: • Una dirección IP privada • Una dirección IP pública
Range	Varias	Traduce un rango de direcciones IP. Consta de lo siguiente: • Una dirección IP privada inicial • Una dirección IP pública inicial • Varias entradas en función del rango especificado
Subnet	1	Traduce todas las direcciones IP de una subred o una de parte de una subred. Consta de lo siguiente: • Una dirección IP privada inicial • Una dirección IP pública inicial alineada con límites de subred válidos • Máscara de subred

EJEMPLO Los siguientes tipos de traducción cuentan como 10 entradas de traducción:

- Traducción de tipo Single para un dispositivo
- Traducción de tipo Range para ocho dispositivos
- Traducción de tipo Subnet para todos los dispositivos de la subred

Los tipos de traducción Single y Range tienen una relación uno a uno entre las entradas de traducción y las direcciones que se van a traducir. Sin embargo, las traducciones de subred tienen una relación uno a muchos, lo que permite una entrada de traducción para muchas direcciones.

Asignaciones de VLAN

Al configurar NAT, puede asignar una o más VLAN a una ocurrencia de NAT. Cuando asigne una VLAN a una ocurrencia de NAT, el tráfico asociado a esa VLAN está sujeto a los parámetros de configuración de la ocurrencia de NAT. Los parámetros de configuración incluyen información sobre si el tráfico se traduce, se corrige, se bloquea o se transfiere.

IMPORTANTE	Configure todos los roles Smartport y las VLAN antes de crear ocurrencias de NAT. Si cambia un rol Smartport o la VLAN nativa de un puerto asociado a una ocurrencia de NAT, deberá volver a asignar las VLAN a la ocurrencia de NAT.

Tenga en cuenta lo siguiente al asignar redes VLAN a una ocurrencia de NAT:

- NAT admite tanto puertos troncales como puertos de acceso.
- NAT no cambia los tags de VLAN.
- Puede asignar un máximo de 128 VLAN a una o más ocurrencias.
- Puede asignar la misma VLAN a varias ocurrencias siempre y cuando la VLAN esté asociada a puertos diferentes. Por ejemplo, puede asignar la VLAN 1 tanto a la ocurrencia A como a la ocurrencia B siempre y cuando la VLAN 1 esté asociada al puerto Gi1/1 de la ocurrencia A y al puerto Gi1/2 de la ocurrencia B.
- De manera predeterminada, cada ocurrencia se asigna a todas las VLAN del puerto Gi1/1 y a ninguna ocurrencia del puerto Gi1/2.

Las VLAN asociadas a un puerto troncal pueden asignarse o no a una ocurrencia de NAT:

- Si se ha asignado una VLAN a una ocurrencia de NAT, su tráfico está sujeto a los parámetros de configuración de la ocurrencia de NAT.

- Si una VLAN no se ha asignado a una ocurrencia de NAT, su tráfico sigue sin traducirse y siempre se permitirá que pase a través del puerto troncal.

Interface de administración y redes VLAN

La interface de administración se puede asociar a una VLAN que se haya asignado o no a una ocurrencia de NAT:

- Si la VLAN asociada se ha asignado a una ocurrencia de NAT, la interface de administración reside en la subred privada de manera predeterminada. Para administrar el switch de la subred privada no es necesario realizar ninguna configuración adicional. Para administrar el switch de la subred pública, debe configurar una traducción de privada a pública.

- Si su VLAN asociada no se ha asignado a una ocurrencia de NAT, el tráfico de la interface de administración sigue sin traducirse y siempre se le permitirá pasar a través del puerto.

Consideraciones acerca de la configuración

Considere estas pautas y limitaciones a la hora de configurar la NAT:

- Un switch solo puede traducir direcciones IPv4.
- Un switch puede tener 128 ocurrencias de NAT como máximo, 128 -VLAN asociadas a la NAT y 128 entradas de traducción. Una traducción de subred cuenta solo como una entrada de traducción, pero incluye traducciones para muchos dispositivos.
- Puede configurar la NAT en uno o ambos puertos de vínculos ascendentes del switch.

IMPORTANTE	Algunas configuraciones de NAT pueden generar cargas de tráfico superiores a las esperadas, tanto en las subredes privadas como en las públicas. También puede estar visible el tráfico no buscado. La NAT no sustituye a un cortafuegos (firewall). Asegúrese de que su configuración sea calificada en cuanto al rendimiento antes de usarla en un ambiente de producción.

Los puertos configurados para NAT **no** admiten lo siguiente al cruzar el límite de NAT debido a las direcciones IP incorporadas que no se hayan corregido, a las direcciones IP cifradas o a la dependencia del tráfico de multidifusión:

- Protocolos de comprobación del cifrado y la integridad del tráfico generalmente incompatibles con NAT, incluido el modo IPsec Transport (módulo 1756-EN2TSC)
- Aplicaciones que usan inicios de sesión dinámicos como, por ejemplo, NetMeeting
- Protocolo de transferencia de archivos (FTP)
- Modelo de objetos componentes distribuido de Microsoft (DCOM), que se usa en comunicaciones de plataforma abierta (OPC)
- Tráfico de multidifusión, incluidas las aplicaciones que usan multidifusión, como CIP Sync (IEEE1588) y redundancia de CLX

Permisos y correcciones de tráfico

Aunque un puerto configurado para NAT puede traducir muchos tipos de tráfico, solo se admiten el tráfico de unidifusión y difusión. Puede optar por bloquear o dejar pasar los siguientes tipos de tráfico que no maneje NAT:

- Tráfico de unidifusión no traducido
- Tráfico de multidifusión
- Tráfico de IGMP

De manera predeterminada, todos los tipos de tráfico anteriores son bloqueados.

Algunos tipos de tráfico se deben corregir para que funcionen correctamente con NAT porque sus paquetes contienen direcciones IP incorporadas. El switch admite correcciones para estos tipos de tráfico:

- Protocolo de resolución de direcciones (ARP)
- Protocolo de mensajes de control de Internet (ICMP)

De manera predeterminada, las correcciones están habilitadas para ARP e ICMP.

Protocolo Ethernet resiliente

El Protocolo Ethernet resiliente (REP) ofrece una alternativa al protocolo de árbol de expansión (STP) para controlar anillos y bucles de red, manejar fallos de vínculos y mejorar el tiempo de convergencia. El REP controla un grupo de puertos conectados en un segmento, garantiza que el segmento no crea ningún bucle de conexión en puente y responde a los fallos de vínculos dentro del segmento. El REP proporciona una base para construir redes más complejas y admite el equilibrio de carga de VLAN.

El REP es un protocolo de segmentos. Un segmento de REP es una cadena de puertos conectados entre sí y configurados con una ID de segmento. Cada segmento consta de puertos de segmentos estándar (Transit) y dos puertos de extremo configurados por el usuario. Un switch puede tener dos puertos como máximo que pertenezcan al mismo segmento, y cada puerto de segmento solo puede tener un vecino externo. Un segmento puede pasar por un medio compartido; sin embargo, en cualquier vínculo, solo dos puertos pueden pertenecer al mismo segmento.
El REP solo se admite en interfaces troncales de capa 2. La selección del switch para Automation Smartport habilita la troncalización de capa 2. El REP se admite en los EtherChannels, pero no en un puerto individual que pertenezca a un EtherChannel.

Puede construir prácticamente cualquier tipo de red basada en segmentos de REP. El REP también admite el equilibrio de cargade VLAN, que se controla mediante el puerto de extremo primario pero que se produce en cualquier puerto del segmento.

Estos tipos de puertos de REP se pueden seleccionar en la interface web del administrador de dispositivos:

- Primary: puerto de extremo primario. Este puerto siempre participa en el equilibrio de carga de VLAN del segmento de REP.

- Edge: puerto de extremo secundario. También participa en el equilibrio de carga de VLAN del segmento de REP.

  Los puertos de extremo son puntos de terminación de un segmento de REP. El usuario debe configurar dos puertos de extremo, incluido un puerto de extremo primario, para cada segmento de REP. La introducción de un extremo sin primario configura el puerto como un puerto de extremo secundario. Los puertos de extremo primarios y secundarios se deben configurar aunque no sea necesaria la compatibilidad con el equilibrio de VLAN.

- Transit: puerto que no es de extremo del segmento de REP.

- No-Neighbor Primary: puerto de extremo primario conectado a un switch sin REP.

- No-Neighbor: puerto de extremo secundario conectado a un switch sin REP.

  Los puertos de extremo No-Neighbor contienen todas las propiedades de los puertos de extremo normales. Estos puertos permiten construir un anillo de REP que incluya un switch no compatible con el protocolo REP.

- None: puerto que no forma parte del segmento de REP.

El REP y el STP pueden coexistir en el mismo switch, pero no en el mismo puerto. El REP no interactúa con el STP. Por ejemplo, si se ha configurado un puerto como un puerto de REP, el STP se inhabilita en ese puerto. Las unidades de datos del protocolo puente (BPDU) del STP no se aceptan en puertos de REP, ni se envían desde dichos puertos. Sin embargo, los anillos o dominios de REP y STP adyacentes pueden compartir un vínculo común. Este vínculo común se puede usar para dejar pasar tráfico del plano de datos de REP y STP, o bien para el tráfico del plano de control de STP.

La Figura 6 muestra un ejemplo de un segmento que consta de seis puertos repartidos por cuatro switches. Los puertos E1 y E2 se configuran como puertos de extremo. Cuando todos los puertos están operativos (como en el segmento de la izquierda), se bloquea un solo puerto, como muestra la línea diagonal. Si se produce un fallo en la red, como se muestra en el diagrama de la derecha, el puerto bloqueado regresa al estado Forwarding para minimizar la perturbación de la red.

Segmento abierto de REP

El segmento que aparece en la Figura 6 es un segmento abierto. No existe conectividad entre los dos puertos de extremo. El segmento de REP no puede originar un bucle de conexión en puente y es seguro conectar los extremos del segmento a cualquier red. Todos los anfitriones conectados a switches dentro del segmento tienen dos posibles conexiones con el resto de la red a través de los puertos de extremo, pero solo se puede obtener acceso a una conexión a la vez. Si un fallo impide que un anfitrión obtenga acceso a su gateway habitual, el REP desbloquea todos los puertos para asegurarse de que esa conectividad está disponible a través del otro gateway.

En el ejemplo siguiente, se pueden configurar E1 o E2 como el puerto de extremo primario.

Figura 6 - Ejemplo de segmento abierto

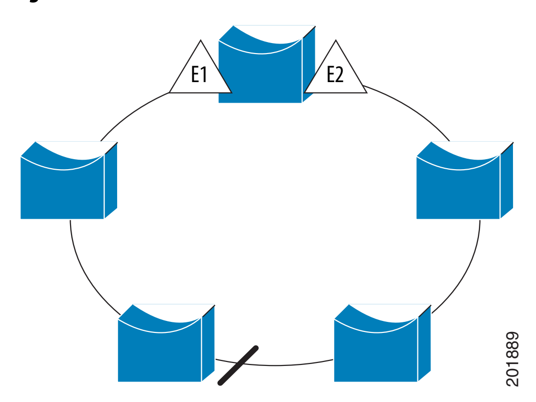
E1 Puerto de extremo
Puerto bloqueado
Fallo de vínculo
E1
E2
E1
E2
201888

Segmento de anillo de REP

El segmento que se muestra en la Figura 7, con ambos puertos de extremo en el mismo switch, es un segmento de anillo. En esta configuración existe conectividad entre los puertos de extremo a través del segmento. Con esta configuración puede crear una conexión redundante entre dos switches cualesquiera del segmento.

En la figura siguiente, se puede configurar E1 o E2 como el puerto de extremo primario.

Figura 7 - Ejemplo de segmento de anillo



Los segmentos de REP tienen estas características:

- Si todos los puertos del segmento están operativos, un puerto (denominado puerto alternativo) está en estado bloqueado para cada VLAN.
- Si se ha configurado el equilibrio de carga de VLAN, dos puertos del segmento controlan el estado bloqueado de las VLAN.
- Si uno o más puertos de un segmento no están operativos, lo cual causa un fallo de vínculo, todos los puertos reenvían tráfico de todas las VLAN para admitir la conectividad en curso.
- En caso de que se produzca un fallo de vínculo, los puertos alternativos se desbloquean lo más rápido posible. Cuando el vínculo fallido vuelve a funcionar normalmente, se selecciona un puerto lógicamente bloqueado por VLAN con una interrupción mínima de la red.

Topologías de anillo de acceso

En las topologías de anillo de acceso, el switch vecino no admite el REP, como se muestra en la Figura 8. En este caso, puede configurar los puertos enfrentados sin REP (E1 y E2) como puertos de extremo no vecinos. Estos puertos heredan todas las propiedades de los puertos de extremo y puede configurarlos igual que cualquier otro puerto de extremo, incluso configurarlos para enviar notificaciones de cambios de topología de STP o REP al switch de agregación. En este caso, la notificación de cambio de topología (TCN) de STP que se envía es un mensaje de STP de árbol de expansión múltiple (MST).

En el ejemplo siguiente, se puede configurar E1 o E2 como puerto primario no vecino.

Figura 8 - Ejemplo de topología de anillo

El REP tiene estas limitaciones:

- Se debe configurar cada puerto del segmento; una configuración incorrecta puede generar bucles de reenvío en las redes.
- El REP puede administrar un solo puerto fallido dentro del segmento; si fallan varios puertos dentro del segmento de REP, se producen pérdidas de conectividad de red.

Configure el REP en redes solo con redundancia. La configuración de REP en una red sin redundancia produce pérdida de conectividad.

Integridad del vínculo

REP no usa un mecanismo de encuestas de extremo a extremo entre los puertos de extremo para verificar la integridad del vínculo. Implementa la detección de fallos del vínculo local. La capa de estado del vínculo (LSL) de REP detecta su vecino compatible con REP y establece la conectividad dentro del segmento. Todas las VLAN están bloqueadas en una interface hasta que se detecta el vecino. Una vez identificado el vecino, el REP determina el puerto vecino que va a convertirse en puerto alternativo y qué puertos van a reenviar el tráfico.

Cada puerto de un segmento tiene una ID de puerto única. El formato de ID de puerto es similar al usado por el algoritmo de árbol de expansión: un número de puerto (único en el puente) asociado a una dirección MAC (única en la red). Cuando el puerto de un segmento se está activando, su LSL empieza a enviar paquetes que incluyen la ID de segmento y la ID de puerto. El puerto se considera operativo cuando realiza un handshake de tres vías con un puerto vecino en el mismo segmento.

SNMP

El switch admite las versiones 1, 2C y 3 del protocolo simple de administración de redes (SNMP). El SNMP permite administrar el switch de manera remota mediante otro software de administración de redes. Esta característica está inhabilitada de manera predeterminada.

El SNMP se basa en tres conceptos:

- Administradores de SNMP (software cliente)
- Agentes de SNMP (dispositivos de red)
- Base de información de administración (MIB)

Consulte MIB admitidas en la página 90 para conocer las MIB admitidas en el switch.

El administrador de SNMP ejecuta el software de administración de SNMP. Los dispositivos de red que se van a administrar, como puentes, encaminadores, servidores y estaciones de trabajo, tienen un módulo de software de agente. El agente proporciona acceso a una MIB local de objetos que refleja los recursos y la actividad del dispositivo. El agente responde también a los comandos del administrador para recuperar los valores de la MIB y definir valores en la MIB. El agente y la MIB están en el switch. Para configurar el SNMP en el switch, se define la relación entre el administrador y el agente.

Tanto SNMPv1 como v2C usan un formato de seguridad basado en la comunidad. Los administradores de SNMP pueden obtener acceso a la MIB de agente mediante contraseñas denominadas cadenas de comunidad. SNMPv1 y v2C se suelen utilizar para el monitoreo de red sin control de red.

SNMPv3 proporciona el monitoreo y control de red. Ofrece un acceso seguro a los dispositivos mediante una combinación de paquetes de cifrado y autenticación a través de la red. El modelo de seguridad utilizado por SNMPv3 es una estrategia de autenticación que se configura para un usuario y para el grupo del usuario. Un nivel de seguridad es el nivel permitido de seguridad dentro de un modelo de seguridad. Una combinación de modelo de seguridad y nivel de seguridad determina el mecanismo de seguridad que se usa para un paquete de SNMP.

A continuación se detallan algunas pautas acerca de los objetos SNMPv3:

IMPORTANTE	SNMPv.3 solo está disponible en la versión criptográfica del firmware del switch.

- Cada usuario pertenece a un grupo.
- Un grupo define la política de acceso para un conjunto de usuarios.
- Una política de acceso define los objetos SNMP a los que se puede tener acceso de lectura, escritura y creación.
- Un grupo determina la lista de notificaciones que pueden recibir sus usuarios.
- Un grupo define también el modelo de seguridad y el nivel de seguridad para sus usuarios.
- Una vista de SNMP es una lista de las MIB a las que puede obtener acceso un grupo.

- Los datos se pueden recopilar de forma segura de los dispositivos SNMP sin temor a que los datos sean alterados o manipulados indebidamente.
- La información confidencial como, por ejemplo, los paquetes de comandos SNMP Set que cambian la configuración de un encaminador, se pueden cifrar para impedir que el contenido quede expuesto en la red.

MIB admitidas

El switch Stratix 5700 admite las siguientes MIB.

Tabla 7 - MIB admitidas

Nombre de la MIB		
BRIDGE-MIB	CISCO-MEMORY-POOL-MIB	IP-MIB
CALISTA-DPA-MIB	CISCO-PAE-MIB	LLDP-EXT-MED-MIB
CISCO-ACCESS-ENVMON-MIB	CISCO-PAGP-MIB	LLDP-MIB
CISCO-ADMISSION-POLICY-MIB	CISCO-PING-MIB	NETRANGER
CISCO-AUTH-FRAMEWORK-MIB	CISCO-PORT-QOS-MIB	NOTIFICATION-LOG-MIB
CISCO-BRIDGE-EXT-MIB	CISCO-PORT-SECURITY-MIB	OLD-CISCO-CHASSIS-MIB
CISCO-BULK-FILE-MIB	CISCO-PORT-STORM-CONTROL-MIB	OLD-CISCO-CPU-MIB
CISCO-CABLE-DIAG-MIB	CISCO-PRIVATE-VLAN-MIB	OLD-CISCO-FLASH-MIB
CISCO-CALLHOME-MIB	CISCO-PROCESS-MIB	OLD-CISCO-INTERFACES-MIB
CISCO-CAR-MIB	CISCO-PRODUCTS-MIB	OLD-CISCO-IP-MIB
CISCO-CDP-MIB	CISCO-RESILIENT-ETHERNET-PROTOCOL-MIB	OLD-CISCO-MEMORY-MIB
CISCO-CIRCUIT-INTERFACE-MIB	CISCO-RTTMON-ICMP-MIB	OLD-CISCO-SYS-MIB
CISCO-CLUSTER-MIB	CISCO-RTTMON-IP-EXT-MIB	OLD-CISCO-SYSTEM-MIB
CISCO-CONFIG-COPY-MIB	CISCO-RTTMON-MIB	OLD-CISCO-TCP-MIB
CISCO-CONFIG-MAN-MIB	CISCO-RTTMON-RTP-MIB	OLD-CISCO-TS-MIB
CISCO-DATA-COLLECTION-MIB	CISCO-SNMP-TARGET-EXT-MIB	RMON-MIB
CISCO-DHCP-SNOOPING-MIB	CISCO-STACK-MIB	RMON2-MIB
CISCO-EMBEDDED-EVENT-MGR-MIB	CISCO-STACKMAKER-MIB	SMON-MIB
CISCO-ENTITY-ALARM-MIB	CISCO-STP-EXTENSIONS-MIB	SNMP-COMMUNITY-MIB
CISCO-ENTITY-VENDORTYPE-OID-MIB	CISCO-SYSLOG-MIB	SNMP-FRAMEWORK-MIB
CISCO-ENVMON-MIB	CISCO-TCP-MIB	SNMP-MPD-MIB
CISCO-ERR-DISABLE-MIB	CISCO-UDLDP-MIB	SNMP-NOTIFICATION-MIB
CISCO-FLASH-MIB	CISCO-VLAN-IFTABLE-RELATIONSHIP-MIB	SNMP-PROXY-MIB
CISCO-FTP-CLIENT-MIB	CISCO-VLAN-MEMBERSHIP-MIB	SNMP-TARGET-MIB
CISCO-IF-EXTENSION-MIB	CISCO-VTP-MIB	SNMP-USM-MIB
CISCO-IGMP-FILTER-MIB	ENTITY-MIB	SNMP-VIEW-BASED-ACM-MIB
CISCO-IMAGE-MIB	ETHERLIKE-MIB	SNMPv2-MIB
CISCO-IP-STAT-MIB	HC-RMON-MIB	TCP-MIB
CISCO-LAG-MIB	IEEE8021-PAE-MIB	UDP-MIB
CISCO-LICENSE-MGMT-MIB	IEEE8023-LAG-MIB	
CISCO-MAC-AUTH-BYPASS-MIB	IF-MIB	
CISCO-MAC-NOTIFICATION-MIB	IP-FORWARD-MIB	

Puerto espejo

El puerto espejo es para usuarios avanzados con experiencia en resolver problemas de tráfico y protocolos en las redes. La característica de puerto espejo copia (o refleja) el tráfico de un puerto en un puerto de monitoreo donde el paquete se puede capturar mediante una herramienta analizadora de protocolos de red. Use el puerto espejo como herramienta de diagnóstico o característica de depuración.

El puerto espejo no afecta la conmutación del tráfico de red en el puerto monitoreado. Debe dedicar un puerto de monitoreo para ser usado como puerto espejo. A excepción del tráfico que se está copiando para la sesión del puerto espejo, el puerto espejo no recibe ni reenvía tráfico.

Puede configurar el puerto espejo asignando el rol Smartport Port Mirroring en un puerto de switch a través de la interface web del administrador de dispositivos.

Encaminamiento

El switch admite estas formas de encaminamiento:

- Static routing: define rutas explícitas entre dos dispositivos (encaminadores y switches). Usted debe definir manualmente la información de encaminamiento, incluida la dirección IP de destino, la máscara de subred de destino y la dirección IP de encaminador del siguiente salto.

- Connected routing: habilita todos los dispositivos de cualquier VLAN que utilicen el switch para comunicarse entre sí si usan el switch como gateway predeterminado. Connected routing se habilita automáticamente si usted habilita Static routing. Para inhabilitar Connected routing e impedir una comunicación entre redes VLAN, debe configurar listas de control de acceso (ACL) mediante la CLI.

La habilitación del encaminamiento es un proceso de dos pasos dentro de la interface web del administrador de dispositivos:

1. Vuelva a asignar memoria del switch para el encaminamiento cambiando la plantilla de administración de bases de datos de switch (SDM) de la plantilla predeterminada a la plantilla Lanbase Routing.
2. Habilite solo Connected routing.

   o bien

   Habilite y configure Static routing, que habilita Connected routing de manera predeterminada.

Administración de la configuración

El switch puede almacenar su configuración en la memoria interna o en una tarjeta SD externa. De manera predeterminada, la tarjeta SD siempre tiene prioridad sobre la memoria interna. Si tiene una imagen IOS y archivos de configuración válidos en la tarjeta SD e inicia el switch con la tarjeta SD insertada, el switch carga los archivos de la tarjeta SD.

En general, el método de inicio del switch se convierte en el origen de los cambios que realice en la configuración. Por ejemplo, si inicia desde la tarjeta SD, cualquier cambio que realice se guardará en la tarjeta SD. Si inicia el switch desde la memoria interna, aunque inserte una tarjeta SD mientras se inicia el sistema, los cambios se guardan en la memoria interna. Para determinar el método de inicio, haga clic en la ficha SD Sync de la interface web del administrador de dispositivos.

Los archivos de configuración (config.text y vlan.dat) tienen un formato ASCII de fácil lectura. Puede descargar los archivos en una computadora mediante uno de estos métodos:
- FTP
- AOP
- Mediante una computadora para leer la tarjeta SD

También puede almacenar los archivos de configuración como parte de su proyecto de controlador en la aplicación Logix Designer.

La interface web del administrador de dispositivos le permite sincronizar su imagen IOS y los archivos de configuración automáticamente o a demanda.

Sincronización de la tarjeta SD

La característica de sincronización de la tarjeta SD le permite sincronizar la tarjeta SD con la memoria flash incorporada. Puede sincronizar los archivos de configuración o la imagen IOS. Si la tarjeta SD está presente, el switch se inicia desde la tarjeta SD con su configuración. Si la tarjeta SD no está presente, el switch lee los parámetros de inicio de la imagen IOS especificada que está almacenada en la memoria interna.

IMPORTANTE	Puede sobrescribir la configuración deseada si realiza la sincronización en la dirección incorrecta.

Alarmas

Puede conectar hasta dos entradas de alarma de dispositivos externos de su ambiente, como una puerta o un indicador de temperatura, al puerto de entrada de alarma del panel frontal del switch. Los contactos de la alarma de salida se pueden configurar mediante la CLI. La salida predeterminada también se activa con una alarma de sobretemperatura o temperatura baja, o una condición de puerto que no reenvía el tráfico. El relé de la alarma de salida se puede configurar como energizado normalmente o como un circuito normalmente desenergizado mediante la CLI.

Software IOS criptográfico (opcional)

El IOS criptográfico de Stratix 5700 (disponible con un número de catálogo independiente para su descarga) proporciona seguridad a la red al cifrar el tráfico de administrador durante las sesiones de Telnet y SNMP. El IOS criptográfico admite todas las características del IOS estándar, así como estos protocolos:

- Protocolo Secure Shell (SSH) v2
- SNMPv3
- HTTPS

Diagnóstico del cable

La característica de diagnóstico del cable le permite ejecutar una prueba en cada puerto de switch para determinar la integridad del cable conectado a los puertos RJ45 (cobre). Esta característica no está disponible para puertos de fibra.

La prueba determina la distancia desde el switch hasta la apertura para cada cable con un valor de error aproximado (más o menos) enumerado de manera individual.

Características de software avanzadas

Hay más características de software avanzadas disponibles, y algunas de ellas se configuran mediante la macro global o los Smartports para las aplicaciones de automatización típicas que se describen en este manual.

Para obtener información acerca de la configuración de características no disponibles en la interface web del administrador de dispositivos o la aplicación Logix Designer, consulte lo siguiente:

- Cisco IE2000 Switch Software Configuration Manual, disponible en http://www.Cisco.com.

- Cisco IE2000 Switch Command-Line Interface Manual, disponible en http://www.Cisco.com.

Notas:

Administración del switch mediante la interface web del administrador de dispositivos

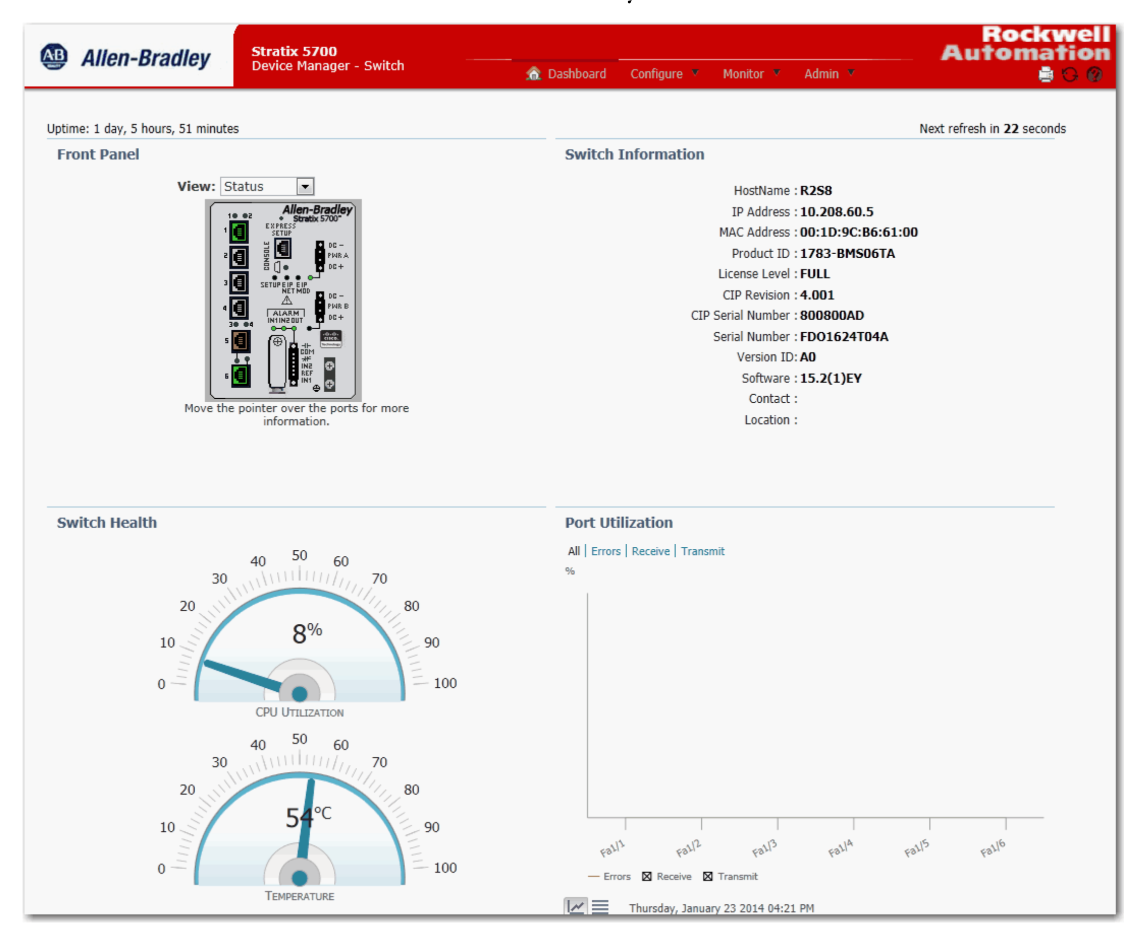
Tras finalizar el proceso de configuración Express Setup, puede administrar el switch utilizando la interface web del administrador de dispositivos que se incluye con el switch.

Por sencillez, la mayoría de las ilustraciones de este capítulo muestran un switch de 6 puertos.

Acceso a la interface web del administrador de dispositivos

Para obtener acceso a la interface web del administrador de dispositivos, siga estos pasos.

1. Abra un navegador web en la estación de trabajo.
2. Escriba la dirección IP del switch en el navegador web y haga clic en Enter.
3. Escriba el nombre de usuario y la contraseña.



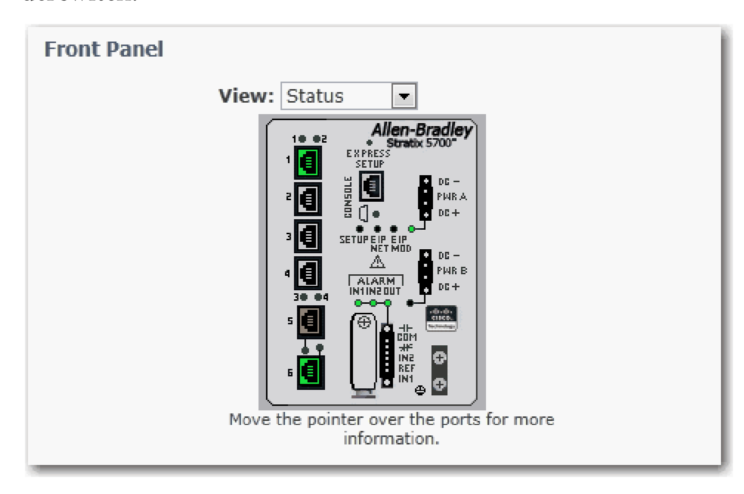
Descripción general del tablero

Puede utilizar el tablero para monitorear el estado y el rendimiento del switch.

La ventana Dashboard es similar a la ventana Monitor > Trends. La ventana Dashboard muestra el estado instantáneo mientras que la ventana Trends muestra el estado histórico. Si se utilizan de manera conjunta, puede determinar el estado detallado del switch y sus puertos. Para obtener información acerca de la ventana Trends, consulte la página 146.

Panel frontal e indicadores de estado

La vista del panel frontal es una representación gráfica de los paneles frontales del switch.



Los componentes del switch que aparecen en la vista del panel frontal están codificados por colores según su estado. Los colores le permiten detectar rápidamente si hay un fallo o una condición de error. -Los indicadores de estado a nivel del sistema y a nivel de los puertos que aparecen en la vista del panel frontal corresponden a los que incluye el switch físico.

Tabla 8 - Indicadores de estado del panel frontal

Indicador	Estado	Descripción
EIP Mod	El indicador de estado EIP Mod muestra el estado del switch.	
	Apagado	La alimentación eléctrica del switch está apagada o no está correctamente conectada.
	Verde fijo	El switch funciona correctamente.
	Verde parpadeante	El switch no está configurado (por ejemplo, el switch no tiene una dirección IP configurada).
	Rojo parpadeante	El switch ha detectado un fallo recuperable del sistema.
	Rojo fijo	El switch ha detectado un fallo no recuperable del sistema.
	Parpadeando en verde y rojo	El switch está realizando su autoprueba de encendido (POST).
DC_A DC_B	Apagado	La alimentación eléctrica del switch está apagada o no está correctamente conectada.
	Verde fijo	La alimentación está presente en el circuito asociado.
	Rojo fijo	La alimentación no está presente en el circuito asociado y el switch se ha configurado para la alimentación de entrada doble.
Alarm Out	Apagado	Salida de alarma no configurada o el switch está apagado.
	Verde fijo	Salida de alarma configurada; no se detecta ninguna alarma.
	Rojo parpadeante	El switch ha detectado una alarma mayor.

Tabla 8 - Indicadores de estado del panel frontal (continuación)

Indicador	Estado	Descripción
Alarm In 1 Alarm In 2	Apagado	Entrada de alarma no configurada.
	Verde fijo	Entrada de alarma configurada; no se detecta ninguna alarma.
	Rojo parpadeante	Alarma mayor detectada.
	Rojo fijo	Alarma menor detectada.
Setup	Apagado	El switch se ha configurado como un switch administrado.
	Verde fijo	El switch está en la configuración inicial.
	Verde parpadeante	El switch está en la configuración inicial, recuperación de fallo o la configuración inicial está incompleta.
	Rojo fijo	El switch no ha podido comenzar la configuración inicial o la recuperación, ya que no hay ningún puerto del switch disponible para conectar con la estación de administración. Desconecte un dispositivo de uno de los puertos del switch y pulse el botón Express Setup del switch.
Puertos: cada puerto combinado tiene dos indicadores de estado: uno para el módulo SFP y otro para el conector RJ45. El indicador de estado adecuado está activo para el puerto activo.		
	Apagado	No hay ningún vínculo presente en el puerto.
	Verde fijo	Vínculo de puerto; sin actividad.
	Verde parpadeante y apagado	El vínculo está activo y funciona correctamente.
	Rojo y ámbar alternante	Hay un fallo o un error en el vínculo.
	Ámbar fijo	El puerto está inhabilitado.
EIP Net: el indicador de estado EIP Net muestra el estado de red del switch.		
	Apagado	La alimentación eléctrica del switch está apagada o no está correctamente conectada.
	Verde fijo	El switch ha establecido una conexión CIP con uno o varios dispositivos conectados.
	Verde parpadeante	El switch tiene una dirección IP pero no ha establecido ninguna conexión con uno o varios dispositivos conectados.
	Rojo parpadeante	Las conexiones de uno o varios dispositivos conectados han sobrepasado el tiempo de espera.
	Rojo fijo	El switch ha detectado que otro dispositivo de la red ya está utilizando su dirección IP.
	Parpadeando en verde y rojo	El switch está realizando su autoprueba de encendido (POST).
Status: en este modo, los indicadores de estado de los puertos muestran el estado de los puertos. Este es el modo predeterminado.		
	Apagado	Sin vínculo.
	Verde fijo	Sin actividad en el vínculo.
	Verde parpadeante	Actividad del vínculo.
	Marrón fijo	Se ha inhabilitado el puerto.
	Amarillo	Un error ha inhabilitado el puerto.
	Parpadeando en verde y ámbar	Vínculo defectuoso.
	Ámbar parpadeante	Desigualdad de configuración de Smartports en el puerto.
	Ámbar fijo	El puerto es defectuoso, se ha inhabilitado a consecuencia de un error o está en estado bloqueado por STP.
Smartports: en este modo, cada imagen de puerto muestra el rol del puerto aplicado. Para obtener información acerca de Smartports, consulte Optimice los puertos mediante roles de puertos Smartport en la página 62.		

Puede cambiar el comportamiento de los indicadores de estado de los puertos eligiendo un modo de puerto desde la lista View de la vista del panel frontal.

Mueva el puntero sobre un puerto para ver información específica acerca de ese puerto y su estado.

SUGERENCIA Si mueve el puntero sobre un puerto que esté parpadeando en verde y ámbar, el estado será uno de los siguientes:
- El vínculo es defectuoso.
- El vínculo tiene colisiones.

En ambos estados, el puerto está recibiendo y enviando tráfico.

Tenga en cuenta lo siguiente:

- La velocidad y el modo duplex de un puerto solo aparecen cuando hay un dispositivo conectado al puerto.
- Para puertos de doble uso, el campo Type muestra 10/100/1000BaseTX para el puerto de vínculo ascendente de cobre independientemente de que el puerto esté activo o no. El campo Type también muestra el tipo del módulo SFP instalado o Empty si no hay ningún módulo instalado.
- El tipo de Smartport, el tipo de VLAN y el nombre aparecen cuando se selecciona el modo Smartport Port.
- El campo Uptime muestra el tiempo que el switch ha estado funcionando desde que se encendió o se reinició la última vez. El estado se actualiza automáticamente cada 60 segundos o al hacer clic en Refresh. El contador de actualización indica el número de segundos que quedan antes de que comience el siguiente ciclo de actualización.

Información del switch

La zona Switch Information del tablero muestra información acerca del switch, tal como se describe en la siguiente tabla.

Campo	Descripción
Host Name	Nombre descriptivo de este switch. El nombre predeterminado es Switch. Puede definir este parámetro en la ventana Admin > Express Setup.
IP Address	Dirección IP de este switch. Puede configurar este ajuste en la ventana Admin > Express Setup.
MAC Address	Dirección MAC de este switch. Esta información no se puede cambiar.
Product ID	Modelo de este switch. Esta información no se puede cambiar.
License Level	Tipo de licencia que se ha instalado. Esta información no se puede cambiar.
CIP Revision	Versión del protocolo industrial común (CIP) que admite este switch. Esta información no se puede cambiar.
CIP Serial Number	Número de serie CIP. Esta información no se puede cambiar.
Serial Number	Número de serie de este switch. Esta información no se puede cambiar.
Version ID	Versión de hardware. Esta información no se puede cambiar.
Software	Versión de IOS que ejecuta este switch. Esta información se actualiza al actualizar el firmware del switch.
Contact	Usuario que es el contacto administrativo de este switch. Puede definir este parámetro en la ventana Configure > SNMP.
Location	Ubicación física de este switch. Puede definir este parámetro en la ventana Configure > SNMP.

Estado del switch

Puede utilizar los medidores de estado para monitorear el switch.

CPU Utilization

El medidor CPU Utilization muestra el porcentaje de la capacidad de procesamiento de la CPU que está utilizando el switch. Los datos se recopilan con la actualización del sistema cada 60 segundos. El medidor cambia a medida que el switch experimenta la actividad de la red generada por los dispositivos que envían datos a través de la red. A medida que aumenta la actividad de la red, también lo hace la competencia entre dispositivos para enviar datos a través de la red.

Al monitorear el uso del switch, observe si el porcentaje de utilización es el esperado durante dicho período de actividad de la red. Si el porcentaje de utilización es alto cuando debería ser bajo, tal vez exista un problema. Al monitorear el switch, observe si la utilización del ancho de banda se mantiene alta continuamente, lo que puede indicar que hay congestión en la red. Si el switch alcanza su ancho de banda máximo (por encima del 90% de utilización) y sus búferes se llenan, comenzará a descartar los paquetes de datos que reciba. No se considera extraño que se pierdan algunos paquetes en la red, y el switch está configurado para ayudar a recuperar los paquetes perdidos, por ejemplo, indicándole a otros dispositivos que vuelvan a enviar los datos. No obstante, una pérdida excesiva de paquetes puede crear errores de paquetes, lo cual puede deteriorar el rendimiento global de la red.

Para reducir la congestión, considere segmentar la red en subredes que estén conectadas mediante otros switches o encaminadores. Investigue si hay otra causa, por ejemplo, conexiones o dispositivos defectuosos, que puedan estar aumentando también la utilización del ancho de banda del switch.

Temperature

El medidor Temperature muestra la temperatura interna del switch. Para obtener información acerca del rango de temperaturas del switch y las pautas sobre el ambiente operativo, consulte el documento Stratix Ethernet Device Specifications Technical Data, publicación 1783-TD001.

Utilización de los puertos

Puede elegir qué tipos de tráfico de la red mostrar y el formato de presentación:

- Tipos de tráfico: de manera predeterminada, se muestra todo el tráfico de todas las interfaces. Haga clic en los vínculos que aparecen encima del área de visualización para ver todo el tráfico, los errores, el tráfico recibido o el tráfico transmitido.

- Formatos: haga clic en los botones ubicados debajo del área de visualización para ver los datos en modo de gráfico o modo de cuadrícula.

- Detalles de los gráficos: mientras consulta un gráfico, coloque el puntero del mouse sobre una barra o un punto del gráfico para ver los datos.

Al monitorear la utilización de los puertos, observe si el porcentaje es el esperado durante dicho período de actividad de la red. Si la utilización es alta cuando debería ser baja, tal vez haya un problema. La asignación del ancho de banda también puede estar basada en si la conexión está funcionando en modo half-duplex o full-duplex.

A continuación se indican algunos de los motivos de los errores recibidos o enviados desde los puertos del switch:
- Mala conexión de los cables
- Puertos defectuosos
- Problemas de software
- Problemas de driver

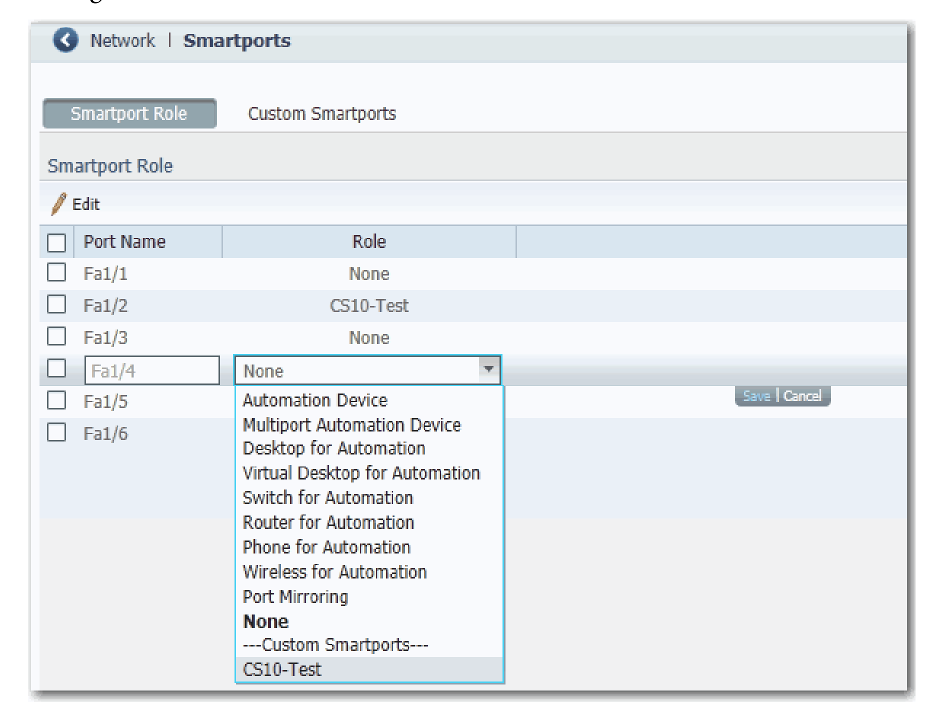
Los datos se recopilan con la actualización del sistema cada 60 segundos.

Consulte Monitoree tendencias en la página 146 para ver un gráfico que muestra los patrones por puerto respecto a las ocurrencias incrementales en función del tiempo (por 60 segundos, 1 hora, 1 día o 1 semana).

Consulte Monitoree estadísticas de puertos en la página 147 para obtener información detallada acerca de los errores de puertos específicos detectados en cada puerto.

Configure Smartports

Para asignar roles Smartport a los puertos del switch, elija Smartports en el menú Configure.



Siga estas pautas cuando utilice roles Smartport:

- Antes de utilizar roles Smartport, decida el tipo de dispositivo que se conectará a cada puerto del switch.
- Antes de conectar un dispositivo al puerto o volver a conectar un dispositivo que se ha trasladado, compruebe el rol Smartport que se ha aplicado a un puerto.

IMPORTANTE	Le recomendamos que no cambie los ajustes de puerto después de habilitar un rol Smartport en un puerto. Cualquier cambio en los ajustes de puerto puede alterar la eficacia del rol Smartport.

- Cuando el usuario intenta aplicar un rol de puerto a un puerto encaminado en la ventana Smartports, aparece el siguiente mensaje de error:

  A port role cannot be configured on a routed port.

Para aplicar un rol Smartport, siga este procedimiento.

1. en el menú Configure, Elija Smartports.
2. Seleccione un puerto.
3. Elija un rol Smartport en el menú desplegable de la columna Role.
4. Haga clic en Save.

Personalice los atributos de los roles de puerto

Cada puerto del switch es un miembro de una VLAN. Los dispositivos conectados a los puertos del switch que pertenecen a una misma VLAN comparten los mismos recursos del sistema y difusiones de datos.

Dependiendo de los requisitos de su red, tal vez baste con asignar todos los puertos a la VLAN predeterminada, cuyo nombre es default. Una VLAN puede bastar para una red pequeña.

Antes de cambiar las afiliaciones a redes de área local virtual (VLAN), debe entender lo que es una VLAN, su finalidad y cómo crearla. Consulte la página 69 para obtener más información sobre las redes VLAN.

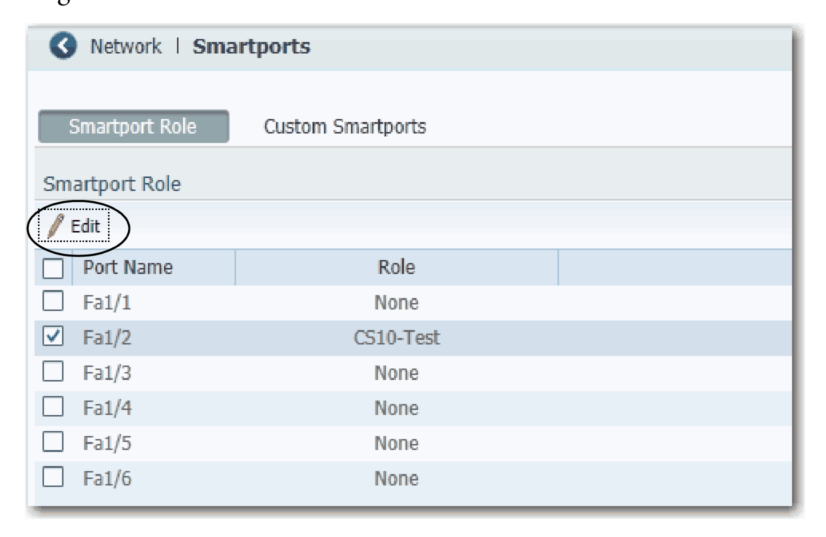
Asigne un puerto a una VLAN (afiliaciones a VLAN)

Cada puerto del switch es un miembro de una VLAN. Los dispositivos conectados a los puertos del switch que pertenecen a una misma VLAN comparten los mismos recursos del sistema y difusiones de datos.
La comunicación entre redes VLAN requiere un dispositivo de capa 3 (como un encaminador o un switch de capa 3).

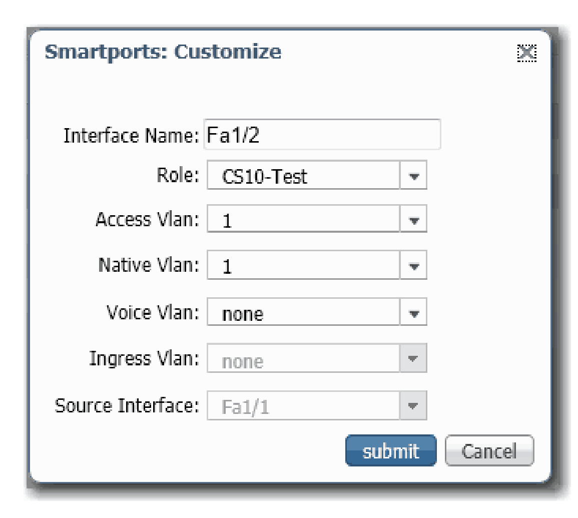
Dependiendo de los requisitos de su red, tal vez baste con asignar todos los puertos a la VLAN predeterminada, cuyo nombre es default. Si se han creado redes VLAN adicionales, deberá decidir cuáles son los puertos que mejor se adaptan a cada VLAN.

Para cambiar una asignación de VLAN, siga estos pasos.

1. En el menú Configure, elija Smartports.
2. Marque la casilla de selección situada junto al puerto cuya VLAN desea cambiar.
3. Haga clic en Edit.



4. Modifique las asignaciones de VLAN según sea necesario:
   - Para puertos que tienen aplicados roles de puerto Automation Device with QoS, Switch For Automation, Router For Automation o Wireless For Automation, elija una VLAN de la lista Native VLAN.
   - Para puertos que tienen aplicados roles de puerto Automation Device, Desktop For Automation, Phone For Automation o None, elija una VLAN de la lista Access VLAN.
   - Para puertos que tienen aplicados el rol de puerto Phone For Automation, elija una VLAN de la lista Voice VLAN.
   - Para puertos que tienen aplicados el rol de puerto Port Mirroring, elija una VLAN de la lista Ingress VLAN y seleccione el puerto que desea monitorear en la lista Source Interface.



5. Haga clic en Submit.

Administre macros personalizadas de Smartport

Para crear una macro personalizada de Smartports, siga estos pasos.

1. Haga clic en la ficha Custom Smartports.
2. Haga clic en Add.
3. Escriba el nombre de la macro.

   En los nombres de las macros se distingue entre mayúsculas y minúsculas. La cadena puede tener hasta 31 caracteres alfanuméricos, que no pueden incluir un signo ?, un espacio ni un tabulador.
4. Elija el icono de la macro (de CS1 a CS10).
5. Escriba la definición de la macro.

   La definición puede contener hasta 3000 caracteres. Escriba los comandos de la macro colocando un comando en cada línea. Utilice el carácter # al comienzo de una línea para escribir un texto de comentario en la macro.

   Los parámetros disponibles para la macro son $native_vlan, $access_vlan y $voice_vlan.

6. Escriba la definición de la antimacro.

   La definición de la antimacro es la parte de la macro aplicada que elimina la macro cuando usted cambia a otra macro o cuando la elimina con el rol Smartport None. Antes de que se pueda aplicar la definición de la macro al puerto, debe definirse primero la antimacro con los comandos adecuados para devolver al puerto su estado original.

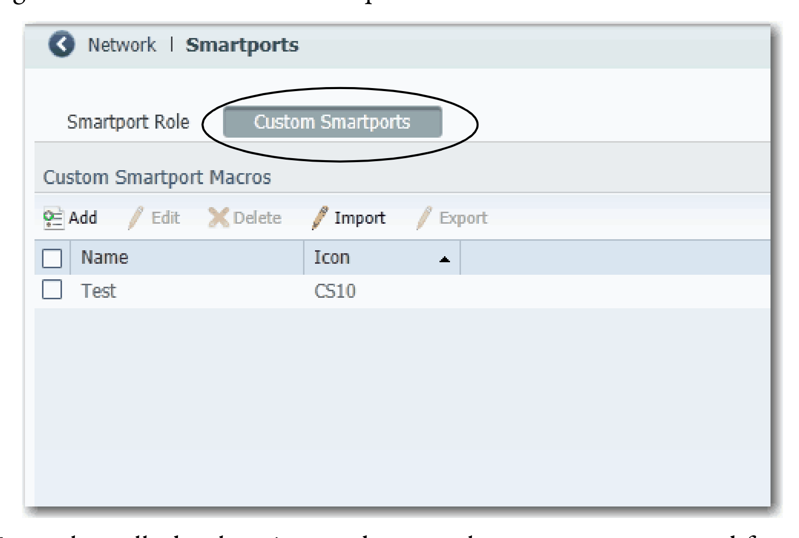
   La definición puede contener hasta 3000 caracteres. Escriba los comandos de la antimacro colocando un comando en cada línea. Utilice el carácter @ para terminar la macro. Utilice el carácter # al comienzo de una línea para escribir un texto de comentario en la macro.

7. Haga clic en Submit.
8. Para descartar todos los cambios que no se hayan guardado, haga clic en Cancel.

Modifique la definición de una macro de Smartports personalizada

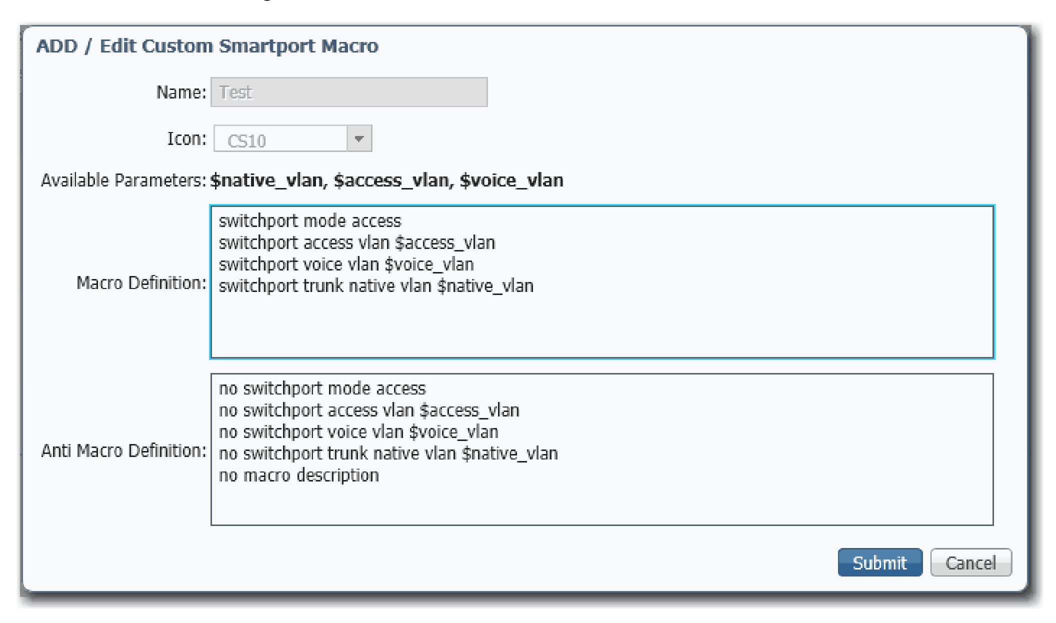
No puede modificar una macro de Smartports personalizada que se esté utilizando actualmente.

1. En el menú Configure, elija Smartports.
2. Haga clic en la ficha Custom Smartports.



3. Marque la casilla de selección situada junto a la macro que quiere modificar.

4. Haga clic en Edit.

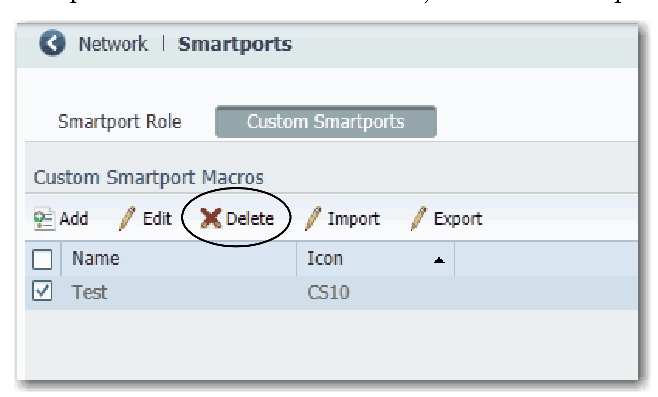


5. Cambie las definiciones según sea necesario.
6. Haga clic en Submit.

Elimine una macro de Smartports personalizada

No puede eliminar una macro de Smartports personalizada que se esté utilizando actualmente.

1. En el menú Configure, elija Smartports.
2. Haga clic en la ficha Custom Smartports.
3. Marque la casilla de selección situada junto a la macro que quiere eliminar.

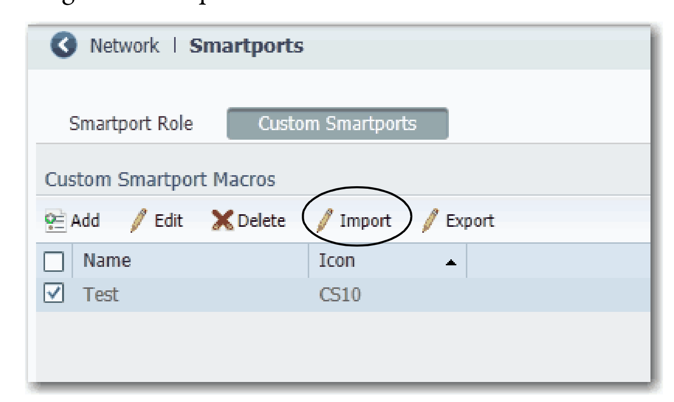


4. Haga clic en Delete.

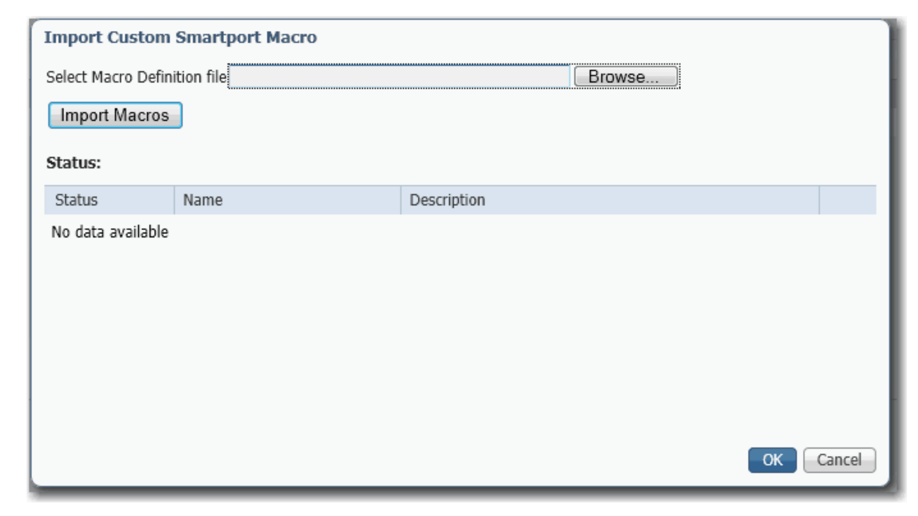
Importe una macro de Smartports personalizada

Debe utilizar Firefox 3.6 o una versión más reciente para importar una macro de Smartports personalizada.

1. En el menú Configure, elija Smartports.
2. Haga clic en la ficha Custom Smartports.
3. Haga clic en Import.



4. Haga clic en Browse.



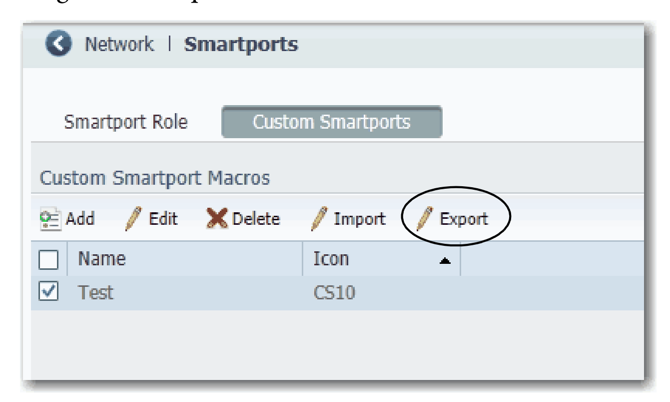
5. Elija el archivo de la macro ubicado en la unidad de almacenamiento de su computadora o de la red.

   El archivo debe ser un archivo .xml con el formato adecuado.
6. Haga clic en Import Macros.
7. Haga clic en OK.

Exporte una macro de Smartports personalizada

Debe utilizar Firefox 3.6 o una versión más reciente para exportar una macro de Smartports personalizada.

1. En el menú Configure, elija Smartports.
2. Haga clic en la ficha Custom Smartports.
3. Marque la casilla de selección situada junto a la macro que quiere exportar.
4. Haga clic en Export.

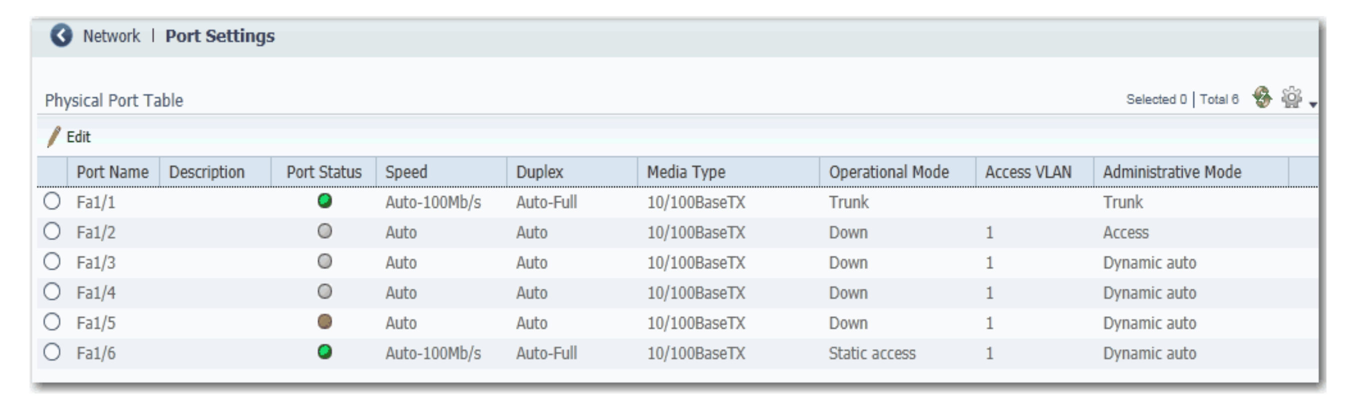


5. Guarde el archivo resultante.

Configure los ajustes de puerto

Los ajustes básicos de puerto determinan la forma en que se reciben y envían datos entre el switch y el dispositivo conectado. Puede cambiar estos ajustes para adaptarlos a las necesidades de su red y resolver problemas de la red. Los ajustes de un puerto del switch deben ser compatibles con los ajustes de puerto del dispositivo conectado.

Para cambiar los ajustes básicos de los puertos, elija Port Settings en el menú Configure.



Port Name	Description	Port Status	Speed	Duplex	Media Type	Operational Mode	Access VLAN	Administrative Mode
Fa1/1			Auto-100Mb/s	Auto-Full	10/100BaseTX	Trunk		Trunk
Fa1/2			Auto	Auto	10/100BaseTX	Down	1	Access
Fa1/3			Auto	Auto	10/100BaseTX	Down	1	Dynamic auto
Fa1/4			Auto	Auto	10/100BaseTX	Down	1	Dynamic auto
Fa1/5			Auto	Auto	10/100BaseTX	Down	1	Dynamic auto
Fa1/6			Auto-100Mb/s	Auto-Full	10/100BaseTX	Static access	1	Dynamic auto

La Tabla 9 muestra los ajustes básicos de los puertos del switch. Para cambiar estos ajustes, haga clic en el botón de radio situado junto al nombre del puerto y haga clic en Edit para abrir la ventana Edit Physical Port.

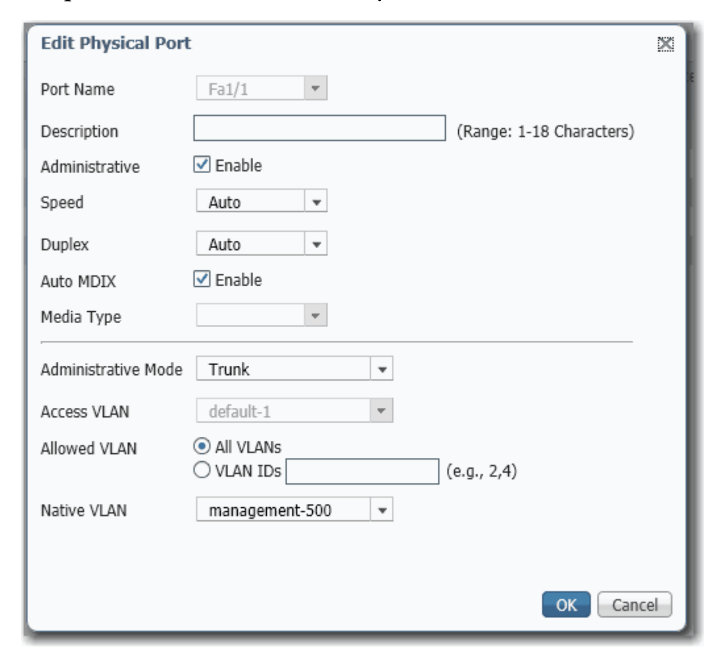


Tabla 9 - Ajustes de puertos

Campo	Descripción
Port Name	Número del puerto del switch, incluido el tipo de puerto, como Fa para Fast Ethernet y Gi para Gigabit Ethernet, y el número de puerto específico: • Gi/1 es el puerto gigabit 1 del switch. • Fa1/1 es el puerto Fast Ethernet 1 del switch.
Description	Descripción del puerto del switch. Recomendamos que proporcione una descripción de puerto que le ayude a identificar el puerto durante el monitoreo y la resolución de problemas. La descripción puede ser la ubicación del dispositivo conectado o el nombre de la persona que utiliza el dispositivo conectado.
Port Status	Estado del puerto del switch. El valor predeterminado es Enabled. Puede cambiar este ajuste en la ventana Edit Physical Port con solo marcar o desmarcar la casilla de selección Administrative. Le recomendamos que inhabilite el puerto si no lo está utilizando y no está conectado a ningún dispositivo. Un ejemplo de una situación en la que se cambia este ajuste es durante la resolución de problemas. Puede inhabilitar administrativamente el puerto para trabajar en un problema relacionado con una conexión bajo sospecha de no estar autorizada.
Speed	Velocidad de funcionamiento del puerto del switch. Puede elegir Auto (autonegociación) si el dispositivo conectado puede negociar la velocidad del vínculo con el puerto del switch. El valor predeterminado es Auto. Le recomendamos que utilice el ajuste predeterminado para hacer coincidir automáticamente la velocidad del puerto del switch con la del dispositivo conectado. Cambie la velocidad del puerto del switch si el dispositivo conectado requiere una velocidad específica. Un ejemplo de una situación en la que se cambia este ajuste es durante la resolución de problemas. Si está resolviendo un problema de conectividad, puede cambiar este ajuste para ver si el puerto del switch y el dispositivo conectado no están ajustados a la misma velocidad.
Duplex	Modo dúplex del puerto del switch: • Auto (autonegociación) si el dispositivo conectado puede negociar con el switch. • Full (modo full-duplex) si ambos dispositivos pueden enviar datos al mismo tiempo. • Half (modo half-duplex) si uno o ambos dispositivos no pueden enviar datos al mismo tiempo. El valor predeterminado es Auto. En los puertos Gigabit Ethernet, no se puede definir el puerto en modo half-duplex si la velocidad del puerto se ha definido en Auto. Le recomendamos que utilice el ajuste predeterminado para hacer coincidir automáticamente el ajuste dúplex del puerto del switch con el del dispositivo conectado. Cambie el modo dúplex del puerto del switch si el dispositivo conectado requiere un modo específico. Un ejemplo de una situación en la que se cambia este ajuste es durante la resolución de problemas. Si está resolviendo un problema de conectividad, puede cambiar este ajuste para ver si el puerto del switch y el dispositivo conectado no están ajustados al mismo modo dúplex.
Auto-MDIX	Determina si la característica automática de conexión cruzada de interface dependiente del medio (Auto-MDIX) puede detectar automáticamente el tipo de conexión de cable que se necesita (conexión directa o conexión cruzada) y configurar la conexión de la forma adecuada. El valor predeterminado es Enable. Este ajuste no está disponible en los puertos de módulo SFP.
Media Type	Tipo de puerto activo (puerto RJ45 o puerto de módulo SFP) de un puerto de vínculo ascendente de doble función. De manera predeterminada, el switch detecta si se ha conectado el puerto RJ45 o el puerto de módulo SFP de un puerto de doble función y utiliza el puerto según corresponda. Solo puede estar activo un puerto al mismo tiempo. Si se conectan ambos puertos, el puerto de módulo SFP tiene prioridad. No se puede cambiar el ajuste de prioridad. Elija entre los siguientes tipos de medios físicos: • SFP: el puerto de módulo SFP está activo. Si elige esta opción, se muestran los ajustes actuales de velocidad y modo dúplex, y Auto-MDIX muestra N/A. • RJ45: el puerto RJ45 está activo. Si elige esta opción, podrá definir los valores de velocidad, modo dúplex y Auto-MDIX del puerto. • Auto (autonegociación): ambos puertos pueden estar activos. Si elige esta opción, la velocidad y el modo dúplex se definen en Auto y Auto-MDIX muestra N/A. El valor predeterminado es Auto.

Tabla 9 - Ajustes de puertos (continuación)

Campo	Descripción
Operational Mode	Estado de operación del puerto. Muestra el modo administrativo o Down (si está inhabilitado).
Access VLAN	VLAN a la que pertenece una interface y para la que transmite tráfico, cuando el vínculo está configurado, o se está comportando, como una interface no troncalizada.
Administrative Mode	Muestra uno de los siguientes modos administrativos: • Access: la interface está en modo no troncalizado permanente y negocia para convertir el vínculo vecino en un vínculo no troncal, incluso si la interface vecina es una interface troncal. Si elige esta opción, seleccione también una VLAN de acceso. Un puerto de acceso pertenece a una sola VLAN y transmite el tráfico de esa única VLAN (a menos que se haya configurado como puerto de VLAN de voz). • Trunk: la interface está en modo troncalizado permanente y negocia para convertir el vínculo vecino en un vínculo troncal, incluso si la interface vecina no es una interface troncal. Si elige esta opción, seleccione también si desea permitir todas las VLAN o solo las ID de VLAN especificadas • Dynamic Auto: la interface convierte el vínculo en un vínculo troncal si la interface vecina está definida en los modos Trunk o Desirable. Este modo es el ajuste predeterminado. Si elige esta opción, especifique la VLAN de acceso que debe utilizarse cuando el vínculo esté en modo Access. Especifique también si desea permitir todas las VLAN o solo las ID de VLAN especificadas cuando el vínculo esté en modo Trunk. • Dynamic Desirable: la interface convierte el vínculo en un vínculo troncal si la interface vecina está configurada en los modos Trunk, Dynamic Desirable o Auto. Si elige esta opción, especifique la VLAN de acceso que debe utilizarse cuando el vínculo esté en modo Access. Elija también si desea permitir todas las VLAN o solo las ID de VLAN especificadas cuando el vínculo esté en modo Trunk.

Configure los umbrales de los puertos

Configure los umbrales de los puertos para evitar que el tráfico de una LAN se vea interrumpido por una tormenta de difusión, multidifusión o unidifusión en una de las interfaces físicas.

Para configurar los umbrales de los puertos, elija Port Thresholds en el menú Configure.

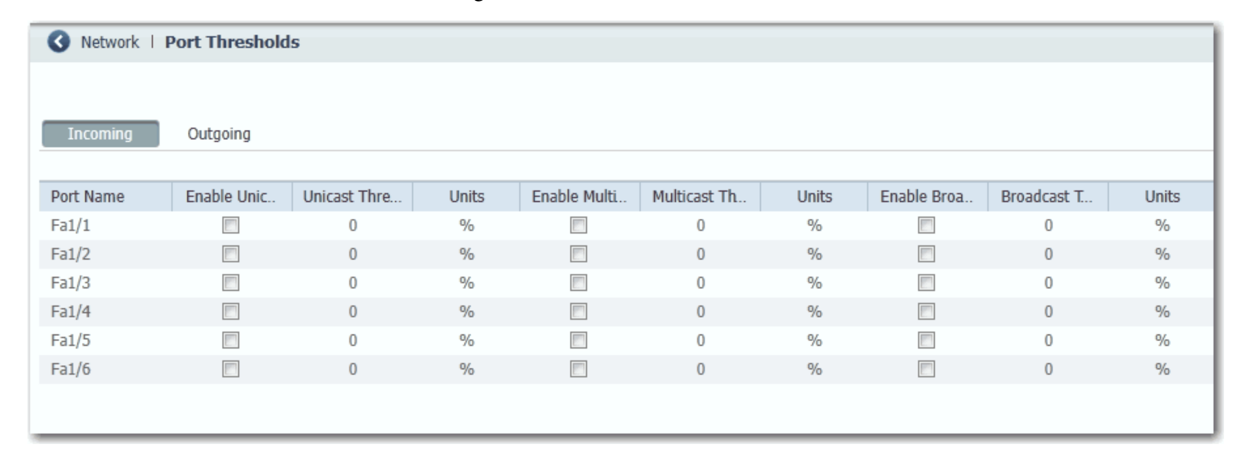


Tabla 10 - Campos de umbrales de los puertos

Campo	Descripción
Incoming	
Unicast	Para cada puerto, haga lo siguiente: 1. Marque o desmarque la casilla de selección Enable. 2. Escriba el valor del umbral. 3. Elija una de estas unidades: – PPS (0…10 mil millones) – BPS (0…10 mil millones) – % (0…100)
Multicast	
Broadcast	
Outgoing	
All Traffic	Para cada puerto, haga lo siguiente: 1. Marque o desmarque la casilla de selección Enable. 2. Escriba el valor del umbral. 3. Haga clic en Save.

Configure EtherChannels

Un EtherChannel, o grupo de puertos, es un grupo de dos o más puertos del switch integrados en un único vínculo lógico para crear un vínculo con un mayor ancho de banda entre dos switches.

Por ejemplo, se pueden asignar cuatro puertos 10/100 de un switch a un EtherChannel para proporcionar un ancho de banda full-duplex de hasta 800 Mb/s. Si uno de los puertos del EtherChannel deja de estar disponible, el tráfico se transmite a través de los puertos restantes del EtherChannel.

Todos los puertos de un EtherChannel deben tener las mismas características:

- Todos se aplican con el rol de puerto Smartports IE Switch y pertenecen a la misma VLAN.
- Todos son puertos 10/100 o todos son puertos 10/100/1000. No se puede agrupar una combinación de puertos 10/100 y 10/100/1000 en un EtherChannel.
- Todos están habilitados. Un puerto inhabilitado de un EtherChannel se trata como un fallo de vínculo y su tráfico se transfiere a uno de los puertos restantes del EtherChannel.

IMPORTANTE	No habilite las direcciones de capa 3 en las interfaces EtherChannel físicas.

Para crear, modificar y eliminar EtherChannels, elija EtherChannels en el menú Configure.

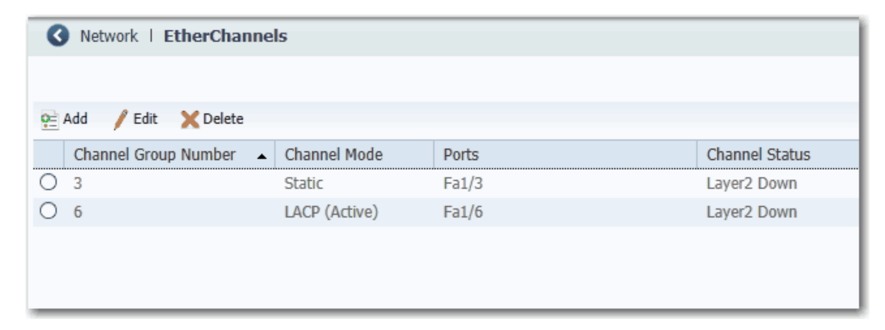


Tabla 11 - Campos de EtherChannel

Campo	Descripción
Channel Group Number	Número de 1 a 6 que identifica este EtherChannel. Puede configurar hasta seis EtherChannels.
Channel Mode	Determina cómo se activan los puertos. Con todas las opciones excepto On, se realizan negociaciones para determinar los puertos que se activan. Los puertos incompatibles se colocan en un estado independiente y siguen transmitiendo tráfico de datos, pero no participan en el EtherChannel. **IMPORTANTE:** Todos los puertos de un EtherChannel deben configurarse con la misma velocidad y modo dúplex. Los modos disponibles son los siguientes: • Static: todos los puertos se unen al EtherChannel, sin negociaciones. Este modo puede resultar útil si el dispositivo remoto no es compatible con los protocolos requeridos por los otros modos (consulte a continuación). Los switches de ambos extremos del vínculo deben configurarse en modo On. • PAgP: este modo habilita el protocolo de agregación de puertos (PAgP), un protocolo de propiedad exclusiva de Cisco. El puerto responde a las solicitudes de creación de EtherChannels pero no inicia estas negociaciones. Se recomienda este modo "silencioso" cuando se conecta un puerto a un dispositivo como, por ejemplo, un servidor de archivos o un analizador de paquetes, que es poco probable que envíe paquetes PAgP. Un puerto en modo Auto puede formar un EtherChannel con otro puerto en el modo Desirable. • PAgP (non-silent): este modo es el mismo que el modo Auto, pero se recomienda cuando se conecta el puerto a un dispositivo que se espera que participe activamente en la iniciación de EtherChannels. Un puerto en modo Auto puede formar un EtherChannel con otro puerto en el modo Desirable. • PAgP Desirable: este modo habilita el protocolo de agregación de puertos (PAgP), un protocolo de propiedad exclusiva de Cisco. El puerto inicia las negociaciones para formar EtherChannels enviando paquetes PAgP a otros puertos. Se recomienda este modo "silencioso" cuando se conecta un puerto a un dispositivo como, por ejemplo, un servidor de archivos o un analizador de paquetes, que es poco probable que envíe paquetes PAgP. Un puerto en modo Desirable puede formar un EtherChannel con otro puerto en el modo Desirable o Auto. • PAgP Desirable (non-silent): este modo es el mismo que el modo Desirable, pero se recomienda cuando se conecta el puerto a un dispositivo que se espera que participe activamente en la iniciación de EtherChannels. • LACP (Active): este modo habilita el protocolo de control de agregación de vínculos (LACP) de manera incondicional. El puerto envía paquetes LACP a otros puertos para iniciar negociaciones a fin de crear EtherChannels. Un puerto en modo Active puede formar un EtherChannel con otro puerto que esté en modo Active o Passive. Los puertos deben configurarse para full-duplex. • LACP (Passive): este modo habilita el protocolo de control de agregación de vínculos solo si se detecta un dispositivo LACP en el otro extremo del vínculo. El puerto responde a las solicitudes de creación de EtherChannels pero no inicia estas negociaciones. Los puertos deben configurarse para full-duplex.
Ports	Puertos que pueden participar en este EtherChannel.
Channel Status	Estado del grupo.

Configure DHCP

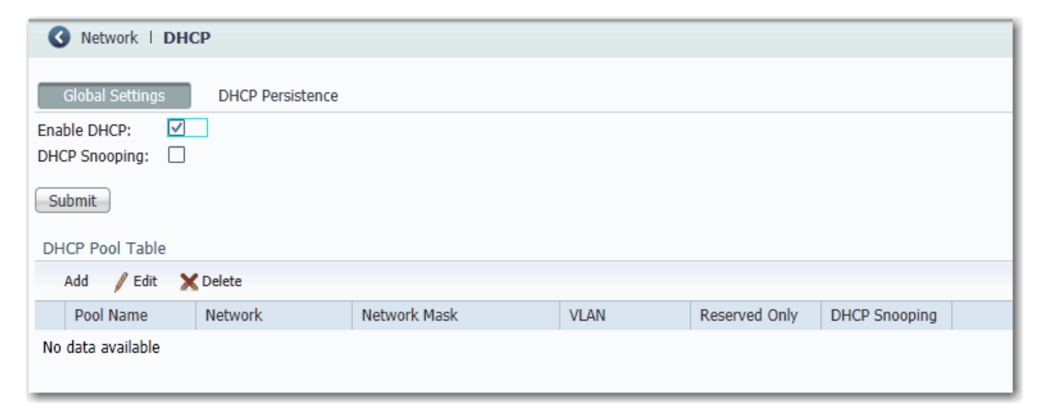
Para utilizar la persistencia de DHCP, primero deberá habilitar DHCP y configurar el grupo de direcciones IP. A continuación, debe asignar una dirección IP específica a cada puerto.

Configure el servidor DHCP

Para habilitar el modo de servidor DHCP en el switch, siga estos pasos.

1. Elija DHCP en el menú Configure.
2. Marque la casilla de selección Enable DHCP.
3. Para habilitar el DHCP Snooping, marque la casilla de selección DHCP Snooping.

   El DHCP Snooping restringe la difusión de peticiones DHCP más allá del switch conectado, lo que significa que los dispositivos recibirán asignaciones de direcciones únicamente del switch conectado. Esta opción solo está disponible en las interfaces de VLAN. Para habilitar DHCP Snooping en una VLAN determinada, marque la casilla de selección DHCP Snooping correspondiente a dicha VLAN en la tabla del grupo de DHCP.



4. Para reservar un grupo de direcciones únicamente para los dispositivos que se han especificado en la tabla de persistencia de DHCP, marque la casilla de selección Reserved Only en la tabla del grupo de DHCP.

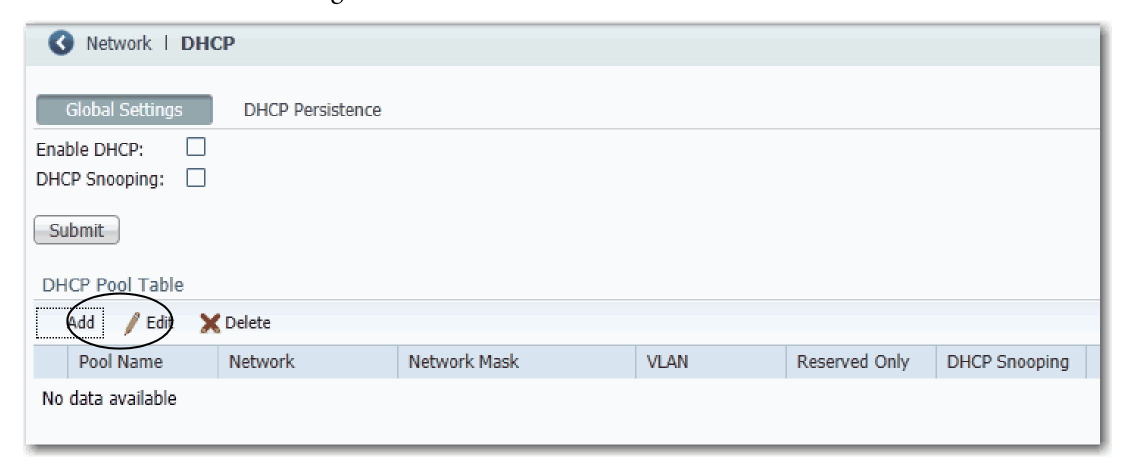
   Se ignorarán las peticiones DHCP procedentes de puertos que no figuren en la tabla de persistencia o que procedan de otro dispositivo (switch). De manera predeterminada, esta opción está inhabilitada y la casilla de selección Reserved Only no está marcada.
5. Haga clic en Submit.

Configure un grupo de direcciones IP de DHCP

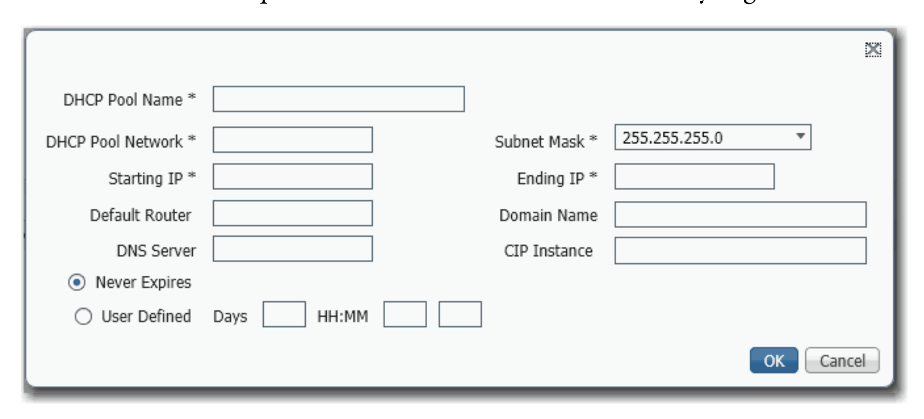
Una vez habilitado el DHCP, puede crear el grupo de direcciones de DHCP.

Para configurar un grupo de direcciones IP de DHCP, siga estos pasos:

1. Elija DHCP en el menú Configure.
2. Haga clic en Add.



3. Rellene los campos tal como se describe a continuación y haga clic en OK.



Campo	Descripción
DHCP Pool Name	Nombre del grupo de direcciones IP de DHCP configurado en el switch. El nombre puede tener un máximo de 31 caracteres alfanuméricos, que no pueden incluir un signo ? ni un tabulador. Este campo es necesario. Un grupo de direcciones IP de DHCP es un rango (o grupo) de direcciones IP disponibles que el switch puede asignar a los dispositivos conectados.
DHCP Pool Network	Dirección IP de la subred del grupo de direcciones IP de DHCP. El formato consiste en una dirección numérica de 32 bits escrita como cuatro números separados por puntos. Cada número puede estar entre 0 y 255. Este campo es necesario.
Subnet Mask	Dirección de red que identifica la subred del grupo de direcciones IP de DHCP. Las subredes segmentan los dispositivos de una red en grupos más pequeños. La máscara predeterminada es 255.255.255.0. Este campo es necesario.
Starting IP	Dirección IP inicial que define el rango de direcciones del grupo de direcciones IP de DHCP. El formato consiste en una dirección numérica de 32 bits escrita como cuatro números separados por puntos. Cada número puede estar entre 0 y 255. Asegúrese de que ninguna de las direcciones IP que asigne se esté usando en otro dispositivo de la red. Este campo es necesario.
Ending IP	Dirección IP final que define el rango de direcciones del grupo de direcciones IP de DHCP. El formato consiste en una dirección numérica de 32 bits escrita como cuatro números separados por puntos. Cada número puede estar entre 0 y 255. Asegúrese de que ninguna de las direcciones IP que asigne se esté usando en otro dispositivo de la red. Este campo es necesario.
Default Router	Dirección IP del encaminador predeterminado correspondiente al cliente DHCP que utiliza este servidor. El formato consiste en una dirección numérica de 32 bits escrita como cuatro números separados por puntos. Cada número puede estar entre 0 y 255.
Domain Name	Nombre de dominio del cliente DHCP. El nombre puede tener un máximo de 31 caracteres alfanuméricos, que no pueden incluir un signo ? ni un tabulador.
DNS Server	Direcciones IP de los servidores de IP del sistema de nombres de dominio (DNS) disponibles para un cliente DHCP. El formato consiste en una dirección numérica de 32 bits escrita como cuatro números separados por puntos. Cada número puede estar entre 0 y 255.
CIP Instance	Número de 1 a 15 que identifica el grupo de direcciones.
[Lease Length]	Duración de la concesión de una dirección IP que se asigna a un cliente DHCP. Haga clic en una de los siguientes: • Never Expires • User Defined Si ha hecho clic en User Defined, escriba la duración de la concesión en términos del número de días, horas y minutos. Esta duración de la concesión se utiliza para todas las asignaciones.

Reserve direcciones IP mediante persistencia de DHCP

Puede reservar y preasignar una dirección IP del grupo de direcciones IP a un puerto específico del switch de manera que el dispositivo conectado a dicho puerto del switch reciba siempre la misma dirección IP independientemente de su dirección MAC.

La persistencia de DHCP resulta útil en redes que se configuran de antemano y en las que existen dependencias relativas a las direcciones IP exactas de algunos dispositivos. Utilice la persistencia de DHCP cuando el dispositivo conectado tenga de desempeñar un rol específico y otros dispositivos sepan su dirección IP. Si se reemplaza el dispositivo, se asignará la misma dirección IP al nuevo dispositivo y no será necesario reconfigurar los demás dispositivos de la red.

Cuando se habilita la característica de persistencia de DHCP, el switch actúa como un servidor DHCP para otros dispositivos de la misma red, incluidos los dispositivos conectados a otros switches. Si el switch recibe una petición DHCP, responderá con cualquier dirección IP de su grupo que no se haya asignado. Para evitar que ocurra esto, marque la casilla Reserve Only de la ventana DHCP, lo que evitará que el switch responda cuando reciba una petición.

Cuando se habilita la persistencia de DHCP en un puerto y se realiza una petición DHCP desde un dispositivo conectado a dicho puerto, el switch asigna la dirección IP correspondiente a ese puerto en la ventana DHCP. También difunde

la petición DHCP al resto de la red. Si hay otro servidor DHCP con direcciones disponibles en la red y recibe esta petición, podría intentar responder, lo que tal vez anule la dirección IP inicial asignada por el switch dependiendo de cómo se comporte el dispositivo final (emplea la primera o la última respuesta de dirección IP). Para evitar que se anule la dirección IP, habilite DHCP Snooping en la VLAN adecuada. Al hacerlo, se bloqueará la difusión de esta petición DHCP, de manera que no responda ningún otro servidor, ni siquiera otro switch Stratix con persistencia de DHCP habilitada.

Si utiliza persistencia de DHCP, le recomendamos que asigne inicialmente direcciones IP estáticas a los dispositivos finales. Si falla un dispositivo final y se sustituye, la característica de persistencia de DHCP asigna una dirección IP de la tabla de persistencia de DHCP. El dispositivo funcionará correctamente con esta dirección IP, pero le recomendamos que reasigne una dirección IP estática a los dispositivos reemplazados.

La figura y la tabla siguientes ilustran el comportamiento de persistencia de DHCP.

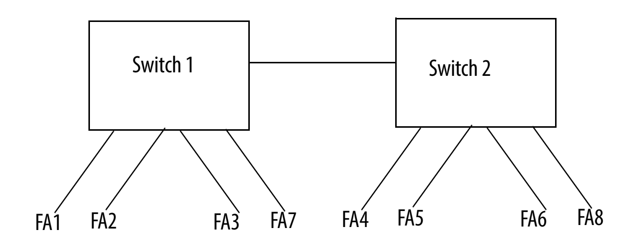


Tabla 12 - Comportamiento de persistencia de DHCP

Si	Significa que
• El switch 1 tiene los puertos FA1…FA3 en su tabla de persistencia • El switch 2 tiene los puertos FA4, FA5, FA6 y FA8 en su tabla de persistencia • No se ha seleccionado Reserve Only y DHCP Snooping está desactivado	Un nuevo dispositivo conectado al switch 1 FA1 recibe una dirección IP de la tabla de persistencia del switch 1. También se envía una petición de difusión a través de la red. El switch 2 responde si hay una dirección no asignada en su grupo, lo que puede anular la asignación realizada por el switch 1.
• El switch 1 tiene los puertos FA1…FA3 en su tabla de persistencia • El switch 2 tiene los puertos FA4, FA5, FA6 y FA8 en su tabla de persistencia • Se ha seleccionado Reserve Only en ambos switches y DHCP Snooping está desactivado	Un nuevo dispositivo conectado al switch 1 FA1 recibe una dirección IP de la tabla de persistencia del switch 1. También se envía una petición de difusión a través de la red. El switch 2 no responde a la petición. Observe que si el dispositivo se conecta al FA7 del switch 1, no recibirá una dirección IP del grupo del switch ya que no está definido en la tabla de persistencia y las direcciones no utilizadas del grupo se bloquean.
• El switch 1 tiene los puertos FA1…FA3 en su tabla de persistencia • El switch 2 tiene los puertos FA4, FA5, FA6 y FA8 en su tabla de persistencia • Se ha seleccionado Reserve Only en el switch 1 y DHCP Snooping está desactivado, pero no el switch 2 cuando DHCP Snooping está desactivado	Un nuevo dispositivo conectado a FA1 recibe una dirección IP de la tabla de persistencia. También se envía una petición de difusión a través de la red. El switch 2 no responde a la petición. Además, un dispositivo conectado a FA4 recibe una dirección IP de la tabla de persistencia del switch 2. Se envía una petición de difusión y el switch 1 responde con una dirección IP no utilizada de su grupo, lo que puede anular el puerto asignado.
• El switch 1 tiene los puertos FA1…FA3 en su tabla de persistencia • El switch 2 tiene los puertos FA4, FA5, FA6 y FA8 en su tabla de persistencia • Se ha seleccionado DHCP Snooping • Se ha marcado Reserved Only	Un nuevo dispositivo conectado al switch 1 FA1 recibe una dirección IP de la tabla de persistencia del switch 1. No se envía una petición de difusión a través de la red, por lo que el switch 2 no responde. Observe que si un dispositivo se conecta al FA7 (no definido en la tabla de persistencia de DHCP) del switch 1, no recibirá una dirección IP del grupo del switch ya que no está definido en la tabla de persistencia y las direcciones no utilizadas del grupo se bloquean.
• El switch 1 tiene los puertos FA1…FA3 en su tabla de persistencia • El switch 2 tiene los puertos FA4, FA5, FA6 y FA8 en su tabla de persistencia • Se ha seleccionado DHCP Snooping • No se ha marcado Reserved Only	Un nuevo dispositivo conectado al switch 1 FA1 recibe una dirección IP de la tabla de persistencia del switch 1. No se envía una petición de difusión a través de la red, por lo que el switch 2 no responde. Observe que si se conecta un dispositivo a FA7 (no definido en la tabla de persistencia de DHCP) del switch 1, recibirá una dirección IP no asignada del grupo del switch 1.

Para asignar, modificar o eliminar una dirección IP de un puerto del switch, haga clic en la ficha DHCP Persistence.

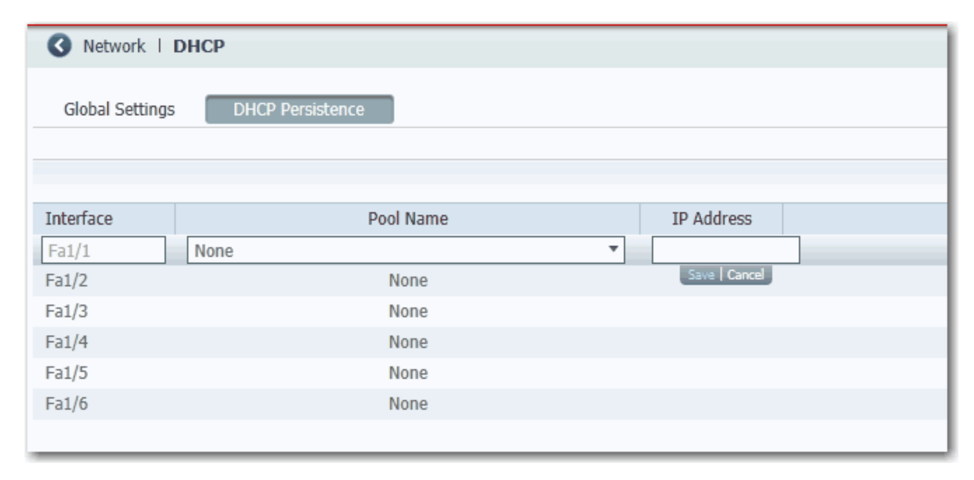
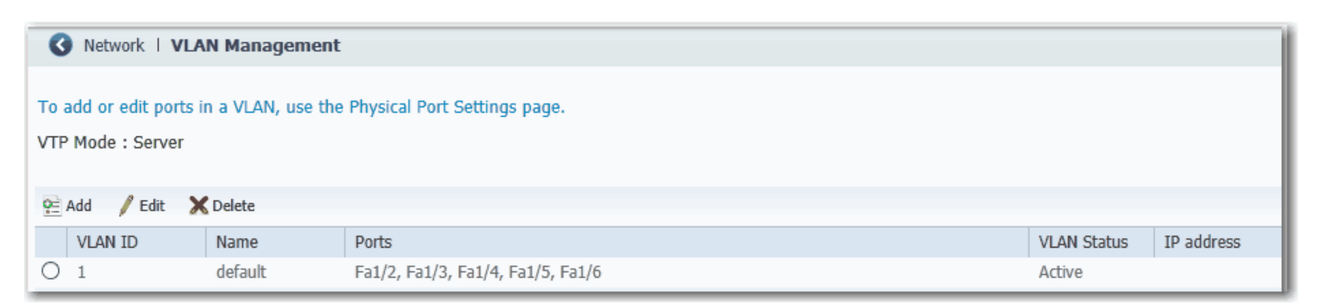


Tabla 13 - Campos de persistencia de DHCP

Campo	Descripción
Interface	Número del puerto del switch, incluido el tipo de puerto (como Fa para Fast Ethernet y Gi para Gigabit Ethernet), y el número de puerto específico. Por ejemplo, Fa1/1 es el puerto Fast Ethernet 1 del switch.
Pool Name	Nombre del grupo de direcciones IP de DHCP configurado en el switch.
IP Address	Dirección IP asignada al puerto del switch. La dirección IP que asigne se reservará para el puerto seleccionado y no estará disponible para la asignación dinámica de DHCP normal. La dirección IP debe ser una dirección del grupo especificado en el campo DHCP Pool Name.

Configure redes VLAN

Para crear, modificar y eliminar redes VLAN, elija VLAN Management en el menú Configure.



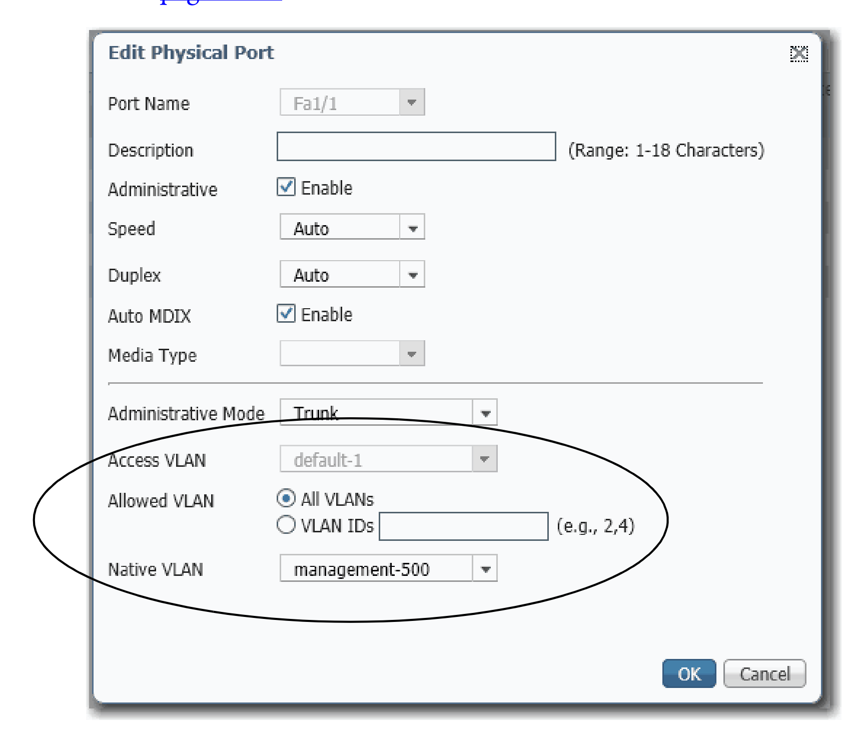
La ID de VLAN predeterminada es 1 y el nombre de la VLAN de administración es default. La VLAN predeterminada por sí sola puede ser suficiente dependiendo del tamaño y los requisitos de su red. Le recomendamos que determine sus necesidades de redes VLAN antes de crear redes VLAN.

Para crear una VLAN, debe indicar un nombre y un número de ID único para la VLAN. Puede modificar el nombre de una VLAN, pero no su número. No puede modificar ni eliminar la VLAN predeterminada.

Tras crear redes VLAN, puede asignar puertos a las VLAN. Antes de asignar puertos a las VLAN, asegúrese de que cada puerto tiene el rol adecuado.

Asigne puertos a VLAN

Para asignar puertos a VLAN, utilice la ventana Edit Physical Ports, según se describe en la página 109.



Configure puertos para alimentación a través de Ethernet (PoE)

Las características PoE y PoE+ son compatibles con los switches con puertos PoE cuando se conecta una fuente de alimentación eléctrica adecuada al switch. Para conocer los requisitos de la fuente de alimentación eléctrica, consulte la página 37.

Puede hacer lo siguiente desde la ventana PoE:

- Limitar la potencia total admitida.
- Configurar los ajustes de modo y de alimentación de los diferentes puertos.

Para la mayoría de las aplicaciones, basta con la configuración predeterminada (modo Auto) y no es necesaria ninguna configuración adicional. No obstante, puede personalizar los ajustes para adaptarlos a sus necesidades. Por ejemplo, para indicar una mayor prioridad de alimentación al puerto PoE, establezca el modo en Static y asigne la alimentación que desee utilizar. Como ejemplo adicional, si no desea que haya dispositivos de alta potencia en un puerto, establezca el modo en Auto y especifique el límite máximo de potencia.

IMPORTANTE Cuando se realizan cambios de configuración PoE en un puerto, se desactiva la alimentación del puerto. La alimentación del puerto se volverá a aplicar dependiendo de la nueva configuración, el estado de los otros puertos PoE y el estado de la provisión de alimentación eléctrica.

Por ejemplo, si el puerto 1 está en modo Auto y en estado On, y lo configura para el modo Static, el switch retirará alimentación eléctrica del puerto 1, detectará el dispositivo alimentado y volverá a alimentar el puerto.

Si el puerto 1 está en modo Auto y en estado On, y lo configura con una potencia máxima de 10 W, el switch retirará la alimentación eléctrica del puerto y seguidamente volverá a detectar el dispositivo alimentado. El switch volverá a alimentar el puerto únicamente si el dispositivo alimentado es un dispositivo clase 1, un dispositivo clase 2 o un dispositivo alimentado exclusivo de Cisco.

Para configurar puertos PoE, elija Power Management en el menú Configure.

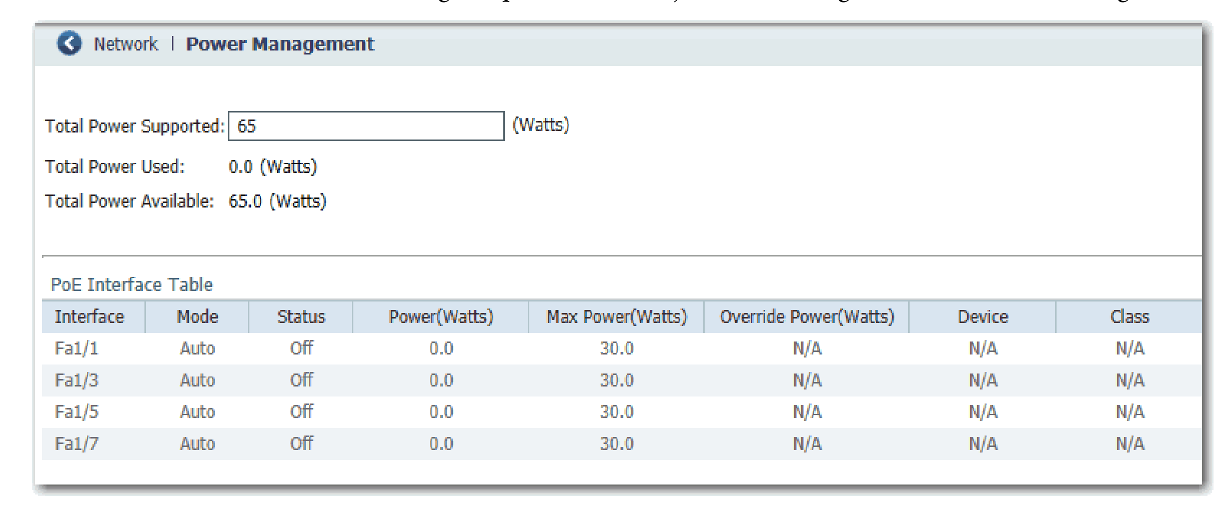


Tabla 14 - Campos de administración de alimentación

Campo	Descripción
Total Power Supported	Para limitar la provisión total de alimentación eléctrica PoE, escriba un valor apropiado en función de la fuente de alimentación eléctrica: • Una fuente de alimentación eléctrica de 48 V suministra un máximo de 65 W. • Una fuente de alimentación eléctrica de 54 V suministra un máximo de 130 W. Al guardar este ajuste, cambiará la provisión total de alimentación eléctrica PoE y se restablecerán los dispositivos alimentados para cumplir con la nueva provisión. **IMPORTANTE:** Una discordancia entre la potencia total admitida y la potencia suministrada puede causar daños al switch. Tenga cuidado de no asignar una potencia mayor que la potencia disponible: • Si planea conectar el switch a una fuente de alimentación eléctrica capaz de entregar una potencia mayor que la configurada, cambie primero la fuente de alimentación y, a continuación, especifique la potencia total admitida. • Si planea conectar el switch a una fuente de alimentación eléctrica capaz de entregar una potencia menor que la configurada, cambie primero la potencia total admitida a un valor adecuado y, a continuación, cambie la fuente de alimentación.
Total Power Used	Muestra la cantidad de potencia que el módulo está utilizando actualmente.
Total Power Available	Muestra la cantidad de potencia no utilizada disponible para el módulo.
Interface	Muestra el número de puerto.
Mode	Muestra el modo de administración de alimentación del puerto: • Auto: habilita la detección de dispositivos alimentados y asigna automáticamente potencia al puerto PoE si hay un dispositivo conectado. Este es el ajuste seleccionado de manera predeterminada. Para limitar la potencia utilizada por este puerto, defina el ajuste Max Power. • Static: reserva potencia para este puerto incluso cuando no haya ningún dispositivo conectado, para asegurarse de que se suministre dicha alimentación cuando se detecte un dispositivo. También puede elegir Static para priorizar un puerto. El switch asignará la potencia a los puertos en modo Static antes de asignarla a los puertos en modo Auto. • Off: PoE está inhabilitado. Para obtener más información, consulte Modos de administración de alimentación eléctrica en la página 66.
Status	Muestra si PoE está habilitado (On) o inhabilitado (Off) en el puerto.
Power (Watts)	Muestra la potencia asignada al puerto.
Max Power (Watts)	Muestra la potencia máxima disponible en el puerto: Puertos PoE: 4…15.4 W Puertos PoE+: 4…30 W
Override Power (Watts)	Indica la anulación de potencia configurada para el puerto. Esta configuración anula tanto la clasificación IEEE que se muestra en la columna Class como la negociación de potencia. Si no se configura ninguna anulación, el campo muestra N/A. La anulación de potencia solo puede configurar mediante la interface de línea de comando (CLI). Para obtener más información, consulte el documento Cisco IE-3000 Software Configuration Guide. **EJEMPLO:** Un administrador puede configurar una anulación cuando se conozca el requisito de potencia de un dispositivo conectado y este sea inferior al valor máximo de la clase. Por ejemplo, si un dispositivo solo requiere 5 W pero pertenece a la clase 0, que permite un máximo de 15.4 W, se puede configurar una anulación para dejar más potencia para los demás dispositivos.
Device	Muestra el dispositivo conectado al puerto. Si no hay ningún dispositivo conectado al puerto, el campo muestra N/A.
Class	Muestra la clasificación de potencia del dispositivo alimentado (PD). Consulte en la Tabla 4 en la página 65 las descripciones de las clasificaciones de potencia.

Configure la sincronización de tiempo de PTP

El estándar IEEE 1588 define un protocolo denominado protocolo de tiempo de precisión (PTP) que permite sincronizar con precisión los relojes de los sistemas de medición y control. Los relojes se comunican entre sí a través de la red de comunicación EtherNet/IP. El protocolo PTP permite que se sincronicen sistemas heterogéneos con relojes de diferente precisión, resolución y estabilidad inherentes. El PTP genera una relación maestro-esclavo entre los relojes del sistema. Todos los relojes obtienen en última instancia su hora de un reloj seleccionado como reloj Grandmaster.

De manera predeterminada, el PTP está inhabilitado en todos los puertos Fast Ethernet y Gigabit Ethernet del switch.

El switch admite los siguientes modos de sincronización de relojes:

- **Modo End-to-End Transparent**: el switch sincroniza de forma transparente todos los relojes esclavos con el reloj maestro conectado al switch.

  El switch corrige el retardo que se produce en cada paquete que atraviesa el switch (denominado tiempo de residencia). Este modo causa menos acumulación de errores y fluctuaciones que el modo Boundary.

  En el modo End-to-End Transparent, todos los puertos del switch están habilitados de manera predeterminada.

- **Modo Boundary**: el switch se convierte en el reloj primario con el que se sincronizan los relojes internos de los otros dispositivos conectados al switch.

  El switch y los dispositivos conectados intercambian constantemente mensajes de temporización para corregir la desviación temporal causada por los offsets de los relojes y los retardos de la red.

  Este modo puede eliminar los efectos de las fluctuaciones de latencia. Dado que la fluctuación y los errores se pueden acumular en las topologías en cascada, utilice este modo solo para redes con menos de cuatro capas de dispositivos en cascada.

  En el modo Boundary, uno o más puertos del switch se pueden habilitar para PTP.

- **Modo Forward (predeterminado)**: el tráfico se reenvía a través del switch (a la vez que se prioriza por QoS), pero el switch no actúa sobre el tráfico.

IMPORTANTE	Cuando cambie los ajustes de los mensajes de temporización de PTP, recuerde que el sistema no funcionará correctamente a menos que todos los dispositivos del sistema tengan los mismos valores.

Para configurar el PTP, elija PTP en el menú Configure.

Una vez que elija un modo, podrá editar los ajustes de cada puerto. Los parámetros dependen del modo seleccionado. Puede configurar el PTP puerto por puerto si el switch está en los modos Boundary o End-to-end Transparent.

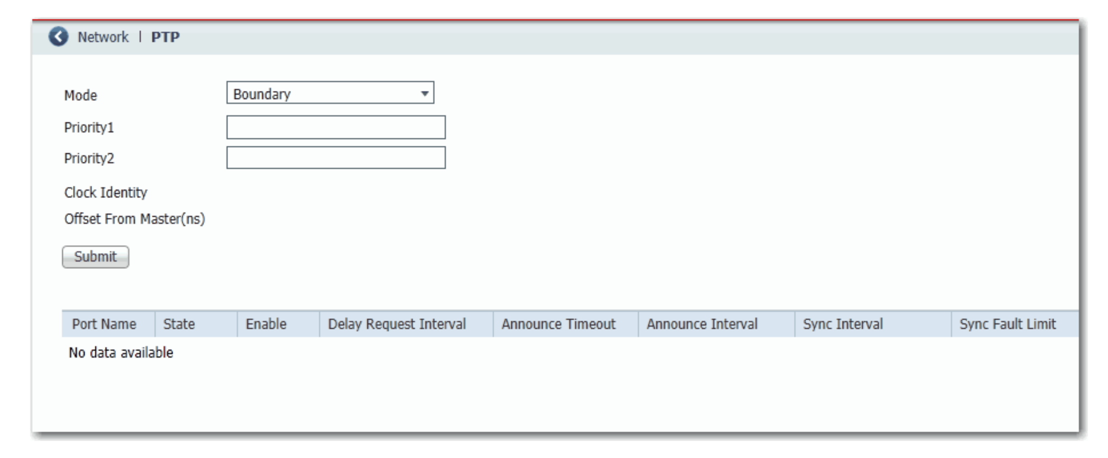


Tabla 15 - Campos de PTP

Campo	Descripción
Mode	Elija un modo de PTP: • Boundary: sincroniza todos los puertos del switch con el reloj Grandmaster utilizando el mecanismo de reloj IEEE 1588 V 2 Boundary. • End-to-End Transparent: calcula y suma el retardo del switch en el paquete del PTP utilizando el mecanismo de reloj IEEE 1588 V2 End-to-End Transparent. En este modo, todos los puertos del switch tienen el PTP habilitado. En el modo Boundary, uno o más puertos del switch se pueden habilitar para el PTP. Puede habilitar o inhabilitar el PTP puerto por puerto. • Forward (predeterminado): transmite los paquetes de PTP sin ninguna interferencia.
Priority 1	Switch utilizado para anular los criterios predeterminados como, por ejemplo, la calidad del reloj o la clase del reloj, para la selección del mejor reloj maestro.
Priority 2	Switch utilizado para desempatar entre dos dispositivos que de otra manera obtendrían la misma valoración según los criterios predeterminados. Por ejemplo, puede dar prioridad a un switch específico respecto a otros switches idénticos. El rango es de 0 a 255. Un valor inferior tiene prioridad. El valor predeterminado es 128.
Clock Identity	Fuente del reloj.
Offset respecto al maestro (ns)	Exactitud en nanosegundos respecto al reloj Grandmaster.
Port Name	Número del puerto del switch, incluido el tipo de puerto (como Fa para Fast Ethernet y Gi para Gigabit Ethernet), el número del switch base (1) y el número de puerto específico. Por ejemplo: Fa1/1 es el puerto Fast Ethernet 1 del switch base.
State	(Solo modo Boundary). Estado de sincronización del puerto del switch con el reloj primario o Grandmaster: • Listening: el puerto del switch está esperando a que se seleccione un reloj primario o Grandmaster. • Pre-master: el puerto del switch está realizando la transición para cambiar al estado Master. • Master: el switch actúa como reloj primario para los dispositivos conectados a dicho puerto del switch. • Passive: el switch ha detectado una ruta redundante a un reloj primario o Grandmaster. Por ejemplo, dos puertos diferentes del switch reclaman el mismo reloj primario o Grandmaster. Para evitar un bucle en la red, el estado de uno de los puertos cambia al estado Passive. • Uncalibrated: el puerto del switch no se puede sincronizar con el reloj primario o Grandmaster. • Slave: el puerto del switch está conectado al reloj primario o Grandmaster y se está sincronizando con él. • Faulty: el PTP no funciona correctamente en ese puerto del switch. • Disabled: el PTP no está habilitado en ese puerto del switch.
Enable	Cuando al menos un puerto del switch está habilitado para PTP, se selecciona de manera predeterminada el modo Forward: Puede habilitar o inhabilitar el PTP puerto por puerto.

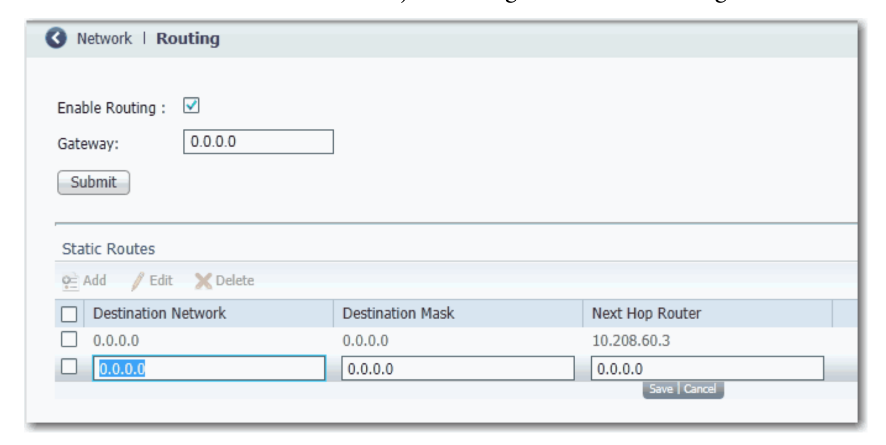
Tabla 15 - Campos de PTP (continuación)

Campo	Descripción
Delay Request Interval	Intervalo de tiempo recomendado al que los dispositivos conectados deben enviar mensajes de petición de retardo cuando el puerto del switch está en el estado Master: • **-1** corresponde a medio segundo • **0** corresponde a 1 segundo • **1** corresponde a 2 segundos • **2** corresponde a 4 segundos • **3** corresponde a 8 segundos • **4** corresponde a 16 segundos • **5** corresponde a 32 segundos • **6** corresponde a 64 segundos El valor predeterminado es 5 (32 segundos).
Announce Timeout	Número de intervalos de anuncio que deben transcurrir sin la recepción de un mensaje de anuncio del reloj Grandmaster antes de que el switch seleccione otro reloj Grandmaster. El número puede estar entre 2 y 10. El valor predeterminado es 3.
Announce Interval	Intervalo de tiempo para enviar mensajes de anuncio: • **0** corresponde a 1 segundo • **1** corresponde a 2 segundos • **2** corresponde a 4 segundos • **3** corresponde a 8 segundos • **4** corresponde a 16 segundos El valor predeterminado es 1 (2 segundos).
Sync Interval	Intervalo de tiempo para enviar mensajes de sincronización: • **-1** corresponde a medio segundo • **0** corresponde a 1 segundo • **1** corresponde a 2 segundos El valor predeterminado es 0 (1 segundo).
Sync Fault Limit	Offset máximo del reloj antes de que el PTP intente readquirir la sincronización. El valor puede estar entre 50 y 500,000,000 nanosegundos. El valor predeterminado es 50,000 nanosegundos. Recomendamos no establecer un límite de sincronización inferior al predeterminado (50,000 nanosegundos). Utilice valores por debajo de 50,000 nanosegundos únicamente en redes con un reloj Grandmaster de muy alta precisión. Estas redes tienen una necesidad crítica de mantener sincronizados dispositivos muy sensibles.

Habilite y configure el encaminamiento

Antes de poder habilitar el encaminamiento, debe reasignar memoria del switch para el encaminamiento, tal como se describe en la página 157.

Para habilitar el encaminamiento, elija Routing en el menú Configure.



En la ventana Routing, puede habilitar solo el encaminamiento conectado, o bien el encaminamiento estático y conectado. Cuando se habilita el encaminamiento estático, el encaminamiento conectado se habilita de manera predeterminada. Para obtener más información acerca de estos tipos de encaminamiento, consulte Encaminamiento en la página 91.

Habilite solo el encaminamiento conectado

Para habilitar solo el encaminamiento conectado, marque Enable Routing y haga clic en Submit.

No se requiere ninguna configuración adicional para el encaminamiento conectado.

Habilite el encaminamiento estático y conectado

Para habilitar el encaminamiento estático y conectado, siga estos pasos.

1. Marque Enable Routing y haga clic en Submit.
2. Configure la información de la ruta estática según se describe a continuación.

Campo	Descripción
Destination Network	Dirección IP del destino.
Destination Mask	Máscara de subred del destino.
Next Hop Router	Dirección IP del encaminador al que este dispositivo enviará los paquetes para el destino especificado.

Configure el STP

Los modos del protocolo de árbol de expansión (STP) incluyen los siguientes:

- El árbol de expansión múltiple (MST) evita los bucles de red al habilitar solo una ruta activa para el tráfico. El MST también proporciona una ruta redundante si la ruta activa deja de estar disponible. Este es el modo STP predeterminado.
- El árbol de expansión por VLAN plus (PVST+) se ejecuta en cada VLAN del switch hasta el máximo admitido, lo que garantiza una ruta sin bucles a través de la red.
- El árbol de expansión rápido por VLAN plus (RPVST+) elimina inmediatamente las direcciones MAC aprendidas dinámicamente al recibir un cambio de la topología. Por el contrario, el PVST+ utiliza un tiempo de envejecimiento breve para las direcciones MAC aprendidas dinámicamente.

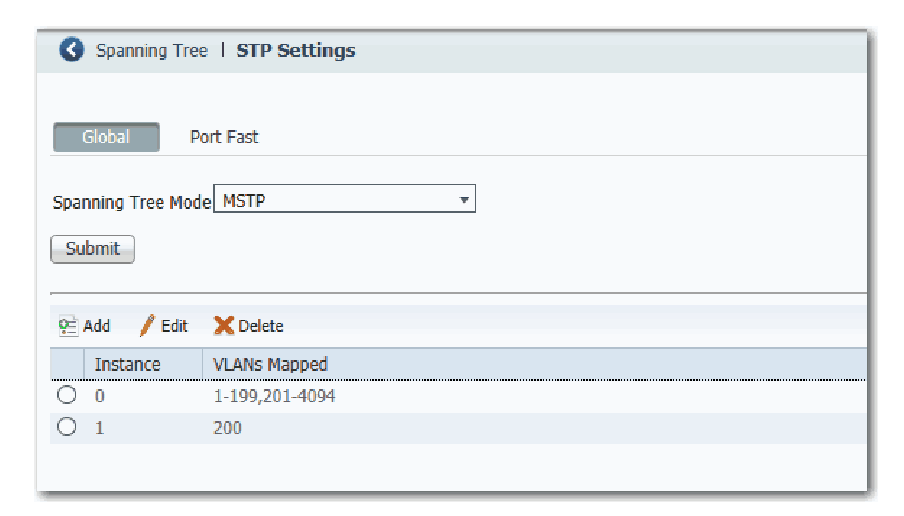
Le recomendamos que deje el STP habilitado para evitar los bucles de red y proporcionar una ruta redundante si la ruta activa deja de estar disponible.

IMPORTANTE Si se inhabilita el STP, la conectividad de la red puede verse afectada.

Para configurar los ajustes del protocolo de árbol de expansión, elija STP en el menú Configure.

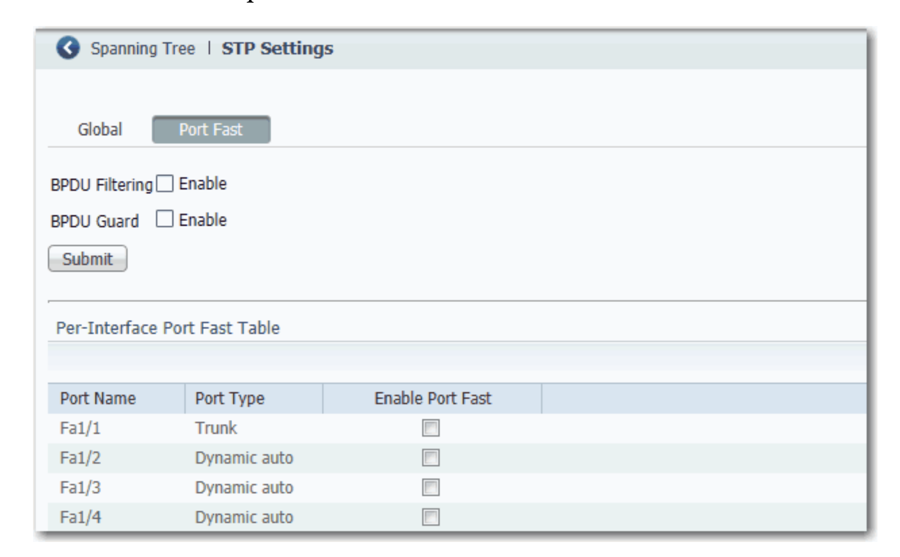
Ajustes globales

Para elegir el modo STP del switch o configurar STP en VLAN individuales, haga clic en la ficha Global. En la ficha Global, puede añadir, editar o eliminar ocurrencias. Si elige los modos PVST+ o Rapid PVST+, puede habilitar o inhabilitar el STP en cada ocurrencia.



Ajustes de PortFast

Para habilitar PortFast y las características relacionadas, haga clic en la ficha PortFast. En la ficha PortFast, puede cambiar la manera en que se implementa el STP en los diferentes puertos.



Las características de PortFast se suelen habilitar únicamente en los puertos de acceso, que se conectan a dispositivos como computadoras personales, puntos de acceso y servidores que no se espera que envíen unidades de datos de protocolo de puente (BPDU). Estas características generalmente no están habilitadas en los puertos que se conectan a switches, ya que pueden producirse bucles en los árboles de expansión.

Características de BPDU

Los switches intercambian tramas especiales denominadas BPDU para comunicar información sobre la red, realizar el seguimiento de los cambios y crear la topología STP. Dado que las BPDU revelan información sobre la red y las BPDU recibidas pueden influir sobre su topología STP, tal vez le resulte útil habilitar BPDU Filtering y BPDU Guard en los puertos de acceso. Estas características impiden que un dispositivo no autorizado pueda interferir en la topología STP. No obstante, le recomendamos que utilice estas características con precaución:

- BPDU Filtering: esta característica de PortFast bloquea completamente el envío y la recepción de las BPDU a través de todos los puertos habilitados para PortFast. Esta característica inhabilita eficazmente STP en estos puertos y pueden producirse bucles. Si se recibe una BPDU, se inhabilita PortFast en el puerto y se aplican los ajustes de STP globales. Para habilitar BPDU Filtering en todos los puertos habilitados para PortFast, marque Enable.

- BPDU Guard: esta característica de PortFast cierra un puerto si recibe una BPDU. Para habilitar BPDU Guard en todos los puertos habilitados para Port Fast, marque Enable.

Observe que si habilita ambas características, BPDU Guard no tendrá ningún efecto ya que BPDU Filtering impedirá que el puerto reciba las BPDU.

Tabla de PortFast por interface

El árbol de expansión requiere una interface para avanzar a través de los estados de escucha y aprendizaje, intercambiar información y establecer una ruta sin bucles antes de que pueda reenviar tramas. En los puertos que conectan con dispositivos como estaciones de trabajo y servidores, puede permitir una conexión inmediata. PortFast efectúa inmediatamente la transición del puerto al modo de reenvío de STP una vez establecido el vínculo.

Para habilitar PortFast en una interface y aplicar las características de BPDU seleccionadas a la interface, seleccione la interface y marque Enable Port Fast.

Configure REP

Para configurar el protocolo Ethernet resiliente (REP), elija REP en el menú Configure.

Para crear un segmento de REP, defina una ID de segmento y un tipo de puerto en los puertos deseados.

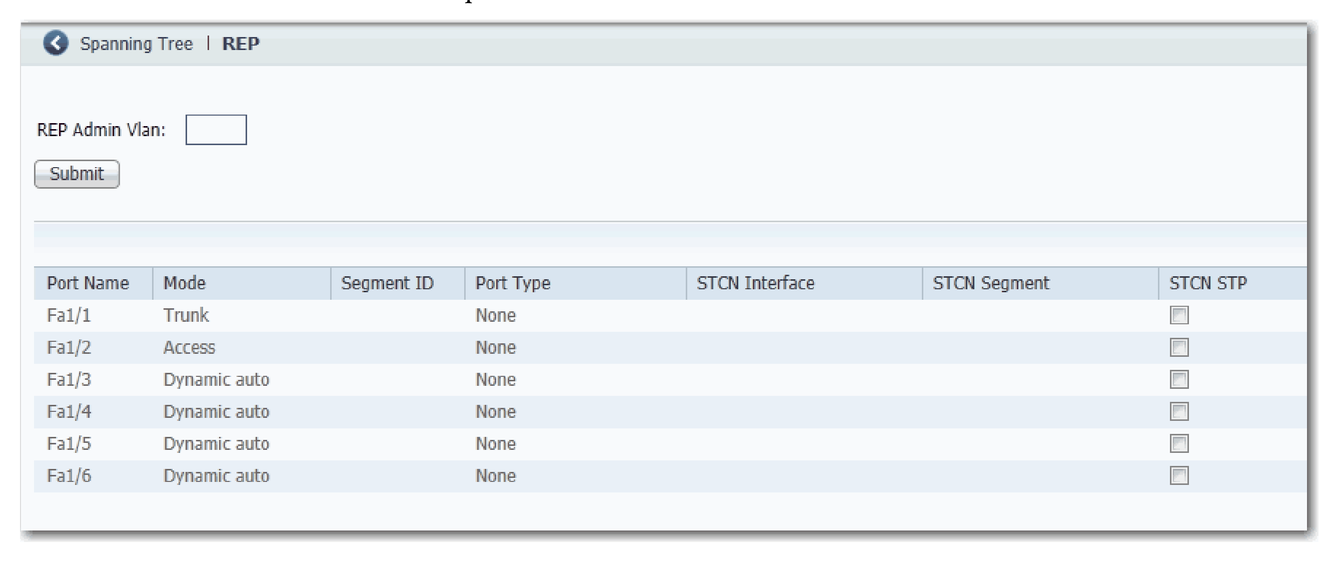


Tabla 16 - Campos de REP

Campo	Descripción
REP Admin VLAN	VLAN administrativa. El rango está entre 2 y 4094. El valor predeterminado es VLAN 1. Los puertos de REP se asignan a la misma VLAN administrativa de REP. Si la VLAN administrativa de REP cambia, se asignarán automáticamente todos los puertos de REP a la nueva VLAN administrativa de REP.
Port Name	Número del puerto del switch, incluido el tipo de puerto (como Fa para Fast Ethernet y Gi para Gigabit Ethernet).
Mode	Modo administrativo. Para definir este modo, elija Port Settings en el menú Configure.
Segment ID	ID del segmento. El rango de ID de segmento está comprendido entre 1 y 1024. Si no se define ninguna ID de segmento, se inhabilita REP.
Port Type	Cada segmento de REP debe tener exactamente dos puertos de extremo primarios y puede tener puertos secundarios que se utilizarán si falla un puerto primario. Puede especificar los puertos primario y secundario preferidos. El configurar un puerto como preferido no garantiza que se convierta en el puerto alternativo, pero se le da una ligera ventaja frente a competidores iguales. También puede indicar que un puerto está conectado a switches no compatibles con REP. Elija uno de los siguientes tipos de puertos: • Edge: un puerto de extremo secundario que participa en el equilibrio de carga de VLAN. • Edge no-neighbor: un puerto de extremo secundario que está conectado a un switch sin REP. • Edge no-neighbor preferred: un puerto de extremo secundario que está conectado a un switch sin REP y es el puerto alternativo preferido para el equilibro de carga de VLAN. • Edge no-neighbor primary: un puerto de extremo secundario que siempre participa en el equilibro de carga de VLAN en este segmento de REP y está conectado a un switch sin REP. • Edge no-neighbor primary preferred: un puerto de extremo que siempre participa en el equilibro de carga de VLAN en este segmento de REP, está conectado a un switch sin REP y es el puerto preferido para el equilibro de carga de VLAN. • Edge preferred: un puerto de extremo secundario que es el puerto alternativo preferido para el equilibro de carga de VLAN. • Edge primary: un puerto de extremo que siempre participa en el equilibro de carga de VLAN en este segmento de REP. • Edge primary preferred: un puerto de extremo que siempre participa en el equilibro de carga de VLAN en este segmento de REP y es el puerto preferido para el equilibro de carga de VLAN. • None: puerto que no forma parte del segmento de REP. El valor predeterminado es None. • Preferred: un puerto de extremo secundario que es el puerto alternativo preferido para el equilibro de carga de VLAN.
STCN Interface	Configure las notificaciones de cambios de topología de segmentos (STCN) de un puerto. El valor predeterminado es None. Las TCN se utilizan en el segmento para notificar a los vecinos del REP los cambios de topología. En el extremo del segmento, el REP puede propagar la notificación al STP o a los otros segmentos del REP.
STCN Segment	Configure las STCN en una ID de segmento. El valor predeterminado es un campo en blanco. Las TCN se utilizan en el segmento para notificar a los vecinos del REP los cambios de topología. En el extremo del segmento, el REP puede propagar la notificación al STP o a los otros segmentos del REP.
STCN STP	Configure las STCN de una red STP. El valor predeterminado corresponde a la casilla de selección no marcada. Las TCN se utilizan en el segmento para notificar a los vecinos del REP los cambios de topología. En el extremo del segmento, el REP puede propagar la notificación al STP o a los otros segmentos del REP.

Configure NAT

Para configurar NAT, siga uno de estos procedimientos según su aplicación:

- Cree ocurrencias de NAT para el tráfico encaminado a través de un encaminador o un switch de capa 3

  Para conocer un ejemplo de esta aplicación, consulte la Figura 4 en la página 81.

- Cree ocurrencias de NAT para el tráfico encaminado a través de un switch de capa 2

  Para conocer un ejemplo de esta aplicación, consulte la Figura 5 en la página 81.

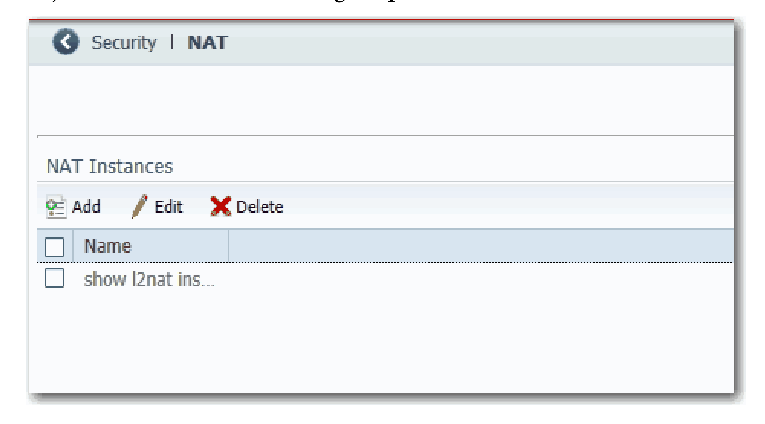
IMPORTANTE	Configure todos los roles Smartport y las VLAN antes de crear ocurrencias de NAT. Si cambia un rol Smartport o la VLAN nativa de un puerto asociado a una ocurrencia de NAT, deberá volver a asignar las VLAN a la ocurrencia de NAT.

IMPORTANTE	Como resultado del reenvío de la capa 2, las sesiones de tráfico actuales permanecen establecidas hasta que sean desconectadas manualmente. Si cambia una traducción existente, deberá desconectar manualmente todas las sesiones de tráfico asociadas antes de que la nueva traducción pueda entrar en vigor.

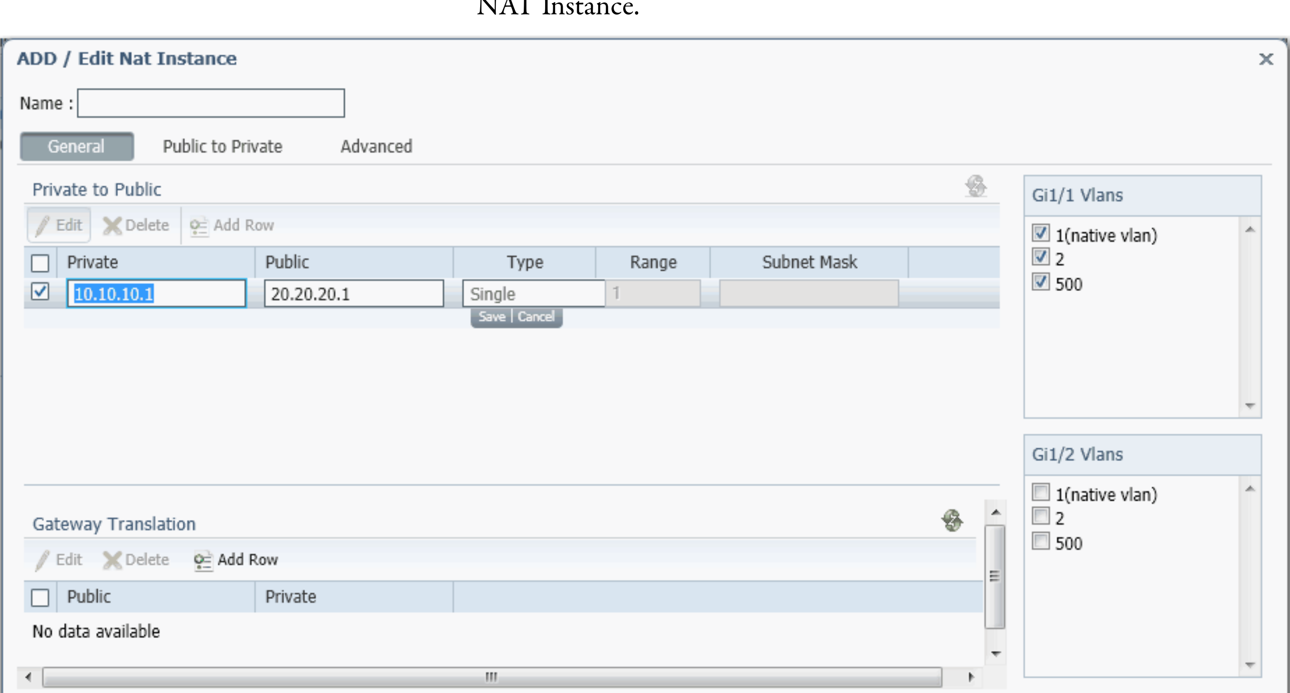
Cree ocurrencias de NAT para el tráfico encaminado a través de un encaminador o un switch de capa 3

Para crear una ocurrencia de NAT para el tráfico encaminado a través de un switch o encaminador de capa 3, siga estos pasos.

1. Elija NAT en el menú Configure para abrir la ventana NAT.



2. Haga clic en Add para ver la ficha General de la ventana Add/Edit NAT Instance.



3. En el campo Name, escriba un nombre único que identifique la ocurrencia.

   El nombre de la ocurrencia no puede incluir espacios ni tener más de 32 caracteres.

4. En la lista de redes VLAN que aparece a la derecha, marque la casilla de selección junto a cada VLAN que quiera asignar a la ocurrencia.

   Para obtener más información acerca de las asignaciones de VLAN, consulte la página 83.

5. En el área Private to Public, haga clic en Add Row, rellene los campos y haga clic en Save.

Campo	Descripción	
Private IP Address	Escriba una dirección IP privada: • Para traducir una sola dirección, escriba la dirección existente del dispositivo en la subred privada. • Para traducir un rango de direcciones, escriba la primera dirección del rango de direcciones consecutivas. • Para traducir las direcciones de una subred, escriba la dirección inicial existente de un dispositivo de la subred privada. Esta dirección debe corresponder al tamaño de la máscara de subred que se desea traducir tal como se muestra a continuación.	
	Máscara de subred	**Dirección inicial de subred privada**
	255.255.0.0	Los últimos dos octetos deben terminar en 0. **EJEMPLO:** 192.168.0.0
	255.255.255.0	El último octeto debe terminar en 0. **EJEMPLO:** 192.168.1.0
	255.255.255.128	El último octeto debe terminar en 0 o 128. **EJEMPLO:** 192.168.1.0 o 192.168.1.128
	255.255.255.192	El último octeto debe terminar en uno de los siguientes: 0, 64, 128, 192. **EJEMPLO:** 192.168.1.64
	255.255.255.224	El último octeto debe terminar en uno de los siguientes: 0, 32, 64, 96, 128, 160, 192, 224. **EJEMPLO:** 192.168.1.32
	255.255.255.240	El último octeto debe terminar en uno de los siguientes: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240. **EJEMPLO:** 192.168.1.16
Public IP Address	Escriba una dirección IP pública: • Para traducir una sola dirección, escriba una dirección pública única que represente el dispositivo. • Para traducir un rango de direcciones, escriba la primera dirección del rango de direcciones consecutivas. • Para traducir direcciones en una subred, escriba una dirección pública inicial única que represente los dispositivos. Esta dirección debe corresponder al tamaño de la máscara de subred que se desea traducir tal como se muestra a continuación.	
	Máscara de subred	**Dirección inicial de subred pública**
	255.255.0.0	Los últimos dos octetos deben terminar en 0. **EJEMPLO:** 10.200.0.0
	255.255.255.0	El último octeto debe terminar en 0. **EJEMPLO:** 10.200.1.0.
	255.255.255.128	El último octeto debe terminar en 0 o 128. **EJEMPLO:** 10.200.1.0 o 10.200.1.128
	255.255.255.192	El último octeto debe terminar en uno de los siguientes: 0, 64, 128, 192. **EJEMPLO:** 10.200.1.64
	255.255.255.224	El último octeto debe terminar en uno de los siguientes: 0, 32, 64, 96, 128, 160, 192, 224. **EJEMPLO:** 10.200.1.32
	255.255.255.240	El último octeto debe terminar en uno de los siguientes: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240. **EJEMPLO:** 10.200.1.16
Type	Elija uno de estos valores: • Single: traduce una sola dirección. • Range: traduce un rango de direcciones. • Subnet: traduce todas las direcciones de la subred privada o una porción de la subred privada.	
Range	Escriba el número de direcciones que desea traducir. Este campo solo estará disponible si se ha elegido Range en el campo Type. Valores válidos: 1…128 Valor predeterminado = 1 **IMPORTANTE:** Cada dirección del rango cuenta como una entrada de traducción. El switch admite un máximo de 128 entradas de traducción.	
Subnet Mask	Escriba la máscara de subred de las direcciones que desea traducir. Valores válidos: • Clase B: 255.255.0.0 • Clase C: 255.255.255.0 • Porción de clase C: – 255.255.255.128 (proporciona 128 direcciones por entrada de traducción) – 255.255.255.192 (proporciona 64 direcciones por entrada de traducción) – 255.255.255.224 (proporciona 32 direcciones por entrada de traducción) – 255.255.255.240 (proporciona 16 direcciones por entrada de traducción)	

6. En el área Gateway Translation, haga clic en Add Row, rellene los campos y haga clic en Save.

   La traducción del gateway permite que los dispositivos de la subred pública se comuniquen con los dispositivos de la subred privada.

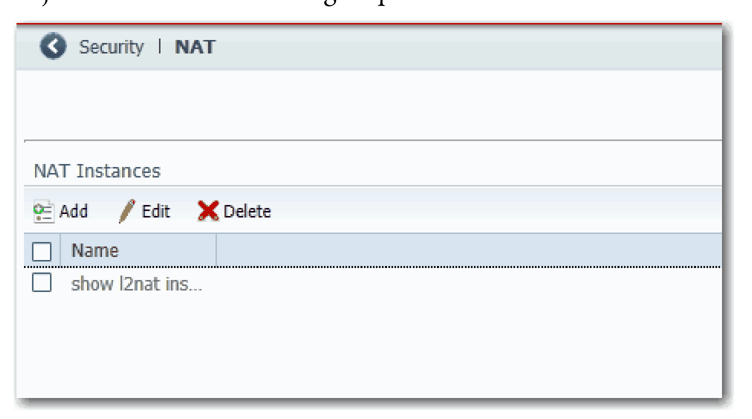
Campo	Descripción
Public	Escriba la dirección del gateway predeterminado del encaminador o switch de capa 3 conectado al puerto de vínculo ascendente del switch.
Private	Escriba una dirección IP única que represente el encaminador o switch de capa 3 en la red privada.

7. (Opcional). Si desea configurar permisos de tráfico y correcciones de paquetes, continúe con Configure permisos y correcciones de tráfico en la página 137.
8. Haga clic en Submit.

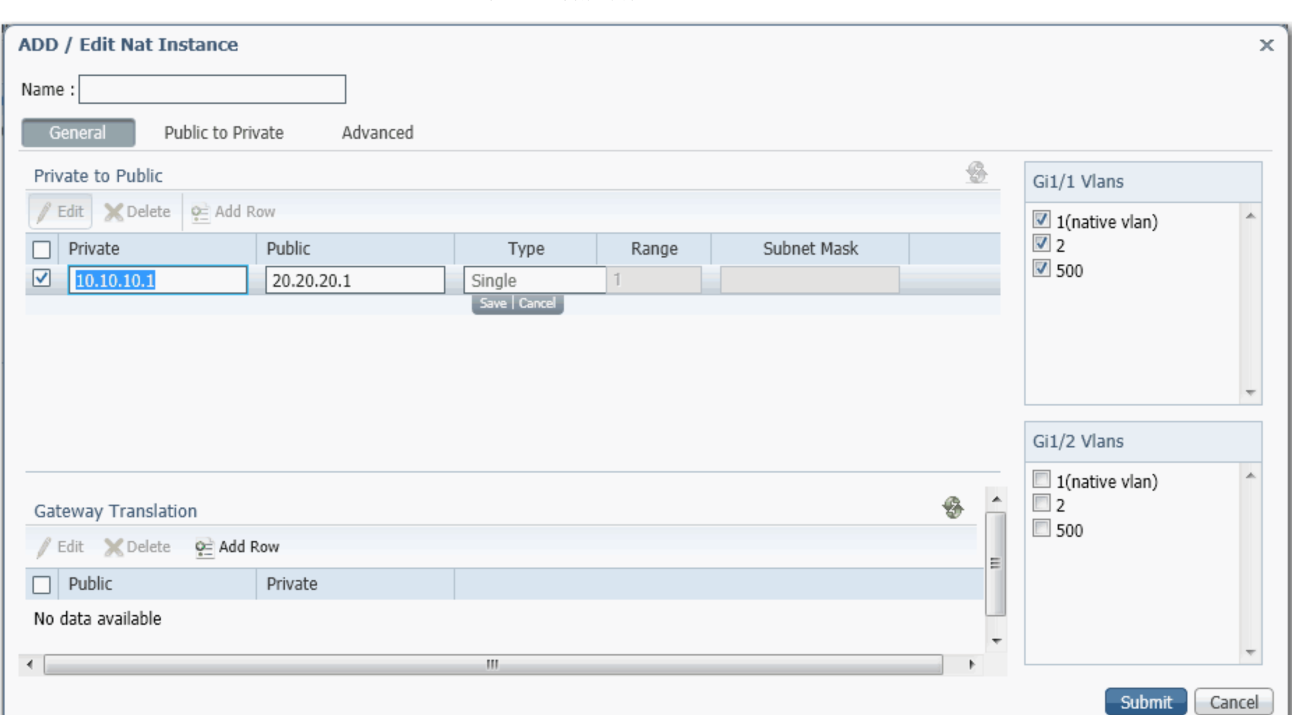
Cree ocurrencias de NAT para el tráfico encaminado a través de un switch de capa 2

Para crear una ocurrencia de NAT para el tráfico encaminado a través de un switch de capa 2, siga estos pasos.

1. Elija NAT en el menú Configure para abrir la ventana NAT.



2. Haga clic en Add para ver la ficha General de la ventana Add/Edit NAT Instance.



3. En el campo Name, escriba un nombre único que identifique la ocurrencia.

   El nombre de la ocurrencia no puede incluir espacios ni tener más de 32 caracteres.

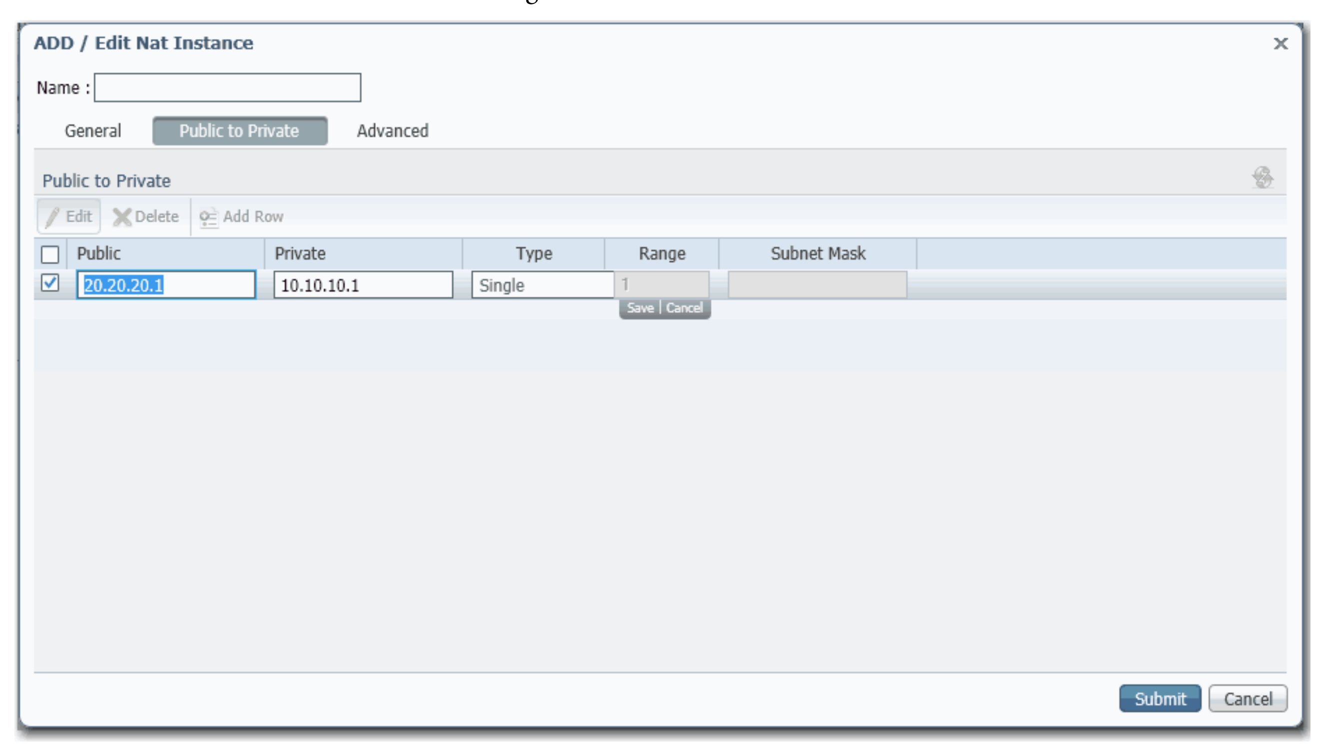
4. En la lista de redes VLAN que aparece a la derecha, marque la casilla de selección junto a cada VLAN que quiera asignar a la ocurrencia.

   Para obtener más información acerca de las asignaciones de VLAN, consulte la página 83.

5. En el área Private to Public, haga clic en Add Row, rellene los campos y haga clic en Save.

<table>
<tr><th>Campo</th><th>Descripción</th></tr>
<tr><td>Private IP Address</td><td>Escriba una dirección IP privada:
• Para traducir una sola dirección, escriba la dirección existente del dispositivo en la subred privada.
• Para traducir un rango de direcciones, escriba la primera dirección del rango de direcciones consecutivas.
• Para traducir las direcciones de una subred, escriba la dirección inicial existente de un dispositivo de la subred privada. Esta dirección debe corresponder al tamaño de la máscara de subred que se desea traducir tal como se muestra a continuación.
<table>
<tr><th>Máscara de subred</th><th>Dirección inicial de subred privada</th></tr>
<tr><td>255.255.0.0</td><td>Los últimos dos octetos deben terminar en 0.
EJEMPLO: 192.168.0.0</td></tr>
<tr><td>255.255.255.0</td><td>El último octeto debe terminar en 0.
EJEMPLO: 192.168.1.0</td></tr>
<tr><td>255.255.255.128</td><td>El último octeto debe terminar en 0 o 128.
EJEMPLO: 192.168.1.0 o 192.168.1.128</td></tr>
<tr><td>255.255.255.192</td><td>El último octeto debe terminar en uno de los siguientes: 0, 64, 128, 192.
EJEMPLO: 192.168.1.64</td></tr>
<tr><td>255.255.255.224</td><td>El último octeto debe terminar en uno de los siguientes: 0, 32, 64, 96, 128, 160, 192, 224.
EJEMPLO: 192.168.1.32</td></tr>
<tr><td>255.255.255.240</td><td>El último octeto debe terminar en uno de los siguientes: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240.
EJEMPLO: 192.168.1.16</td></tr>
</table></td></tr>
<tr><td>Public IP Address</td><td>Escriba una dirección IP pública:
• Para traducir una sola dirección, escriba una dirección pública única que represente el dispositivo.
• Para traducir un rango de direcciones, escriba la primera dirección del rango de direcciones consecutivas.
• Para traducir direcciones en una subred, escriba una dirección pública inicial única que represente los dispositivos. Esta dirección debe corresponder al tamaño de la máscara de subred que se desea traducir tal como se muestra a continuación.
<table>
<tr><th>Máscara de subred</th><th>Dirección inicial de subred pública</th></tr>
<tr><td>255.255.0.0</td><td>Los últimos dos octetos deben terminar en 0.
EJEMPLO: 10.200.0.0</td></tr>
<tr><td>255.255.255.0</td><td>El último octeto debe terminar en 0.
EJEMPLO: 10.200.1.0.</td></tr>
<tr><td>255.255.255.128</td><td>El último octeto debe terminar en 0 o 128.
EJEMPLO: 10.200.1.0 o 10.200.1.128</td></tr>
<tr><td>255.255.255.192</td><td>El último octeto debe terminar en uno de los siguientes: 0, 64, 128, 192.
EJEMPLO: 10.200.1.64</td></tr>
<tr><td>255.255.255.224</td><td>El último octeto debe terminar en uno de los siguientes: 0, 32, 64, 96, 128, 160, 192, 224.
EJEMPLO: 10.200.1.32</td></tr>
<tr><td>255.255.255.240</td><td>El último octeto debe terminar en uno de los siguientes: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240.
EJEMPLO: 10.200.1.16</td></tr>
</table></td></tr>
<tr><td>Type</td><td>Elija uno de estos valores:
• Single: traduce una sola dirección.
• Range: traduce un rango de direcciones.
• Subnet: traduce todas las direcciones de la subred privada o una porción de la subred privada.</td></tr>
<tr><td>Range</td><td>Escriba el número de direcciones que desea traducir. Este campo solo estará disponible si se ha elegido Range en el campo Type.
Valores válidos: 1…128
Valor predeterminado = 1
IMPORTANTE: Cada dirección del rango cuenta como una entrada de traducción. El switch admite un máximo de 128 entradas de traducción.</td></tr>
<tr><td>Subnet Mask</td><td>Escriba la máscara de subred de las direcciones que desea traducir.
Valores válidos:
• Clase B: 255.255.0.0
• Clase C: 255.255.255.0
• Porción de clase C:
– 255.255.255.128 (proporciona 128 direcciones por entrada de traducción)
– 255.255.255.192 (proporciona 64 direcciones por entrada de traducción)
– 255.255.255.224 (proporciona 32 direcciones por entrada de traducción)
– 255.255.255.240 (proporciona 16 direcciones por entrada de traducción)</td></tr>
</table>

6. Haga clic en la ficha Public to Private.



7. Haga clic en Add Row, rellene los campos y haga clic en Save.

<table>
<tr><th>Campo</th><th>Descripción</th></tr>
<tr><td>Public IP Address</td><td>Escriba una dirección IP pública:
• Para traducir una sola dirección, escriba la dirección existente del dispositivo en la subred pública.
• Para traducir un rango de direcciones, escriba la primera dirección del rango de direcciones consecutivas.
• Para traducir las direcciones de una subred, escriba la dirección inicial existente del rango de dispositivos de la subred pública. Esta dirección debe corresponder al tamaño de la máscara de subred que se desea traducir tal como se muestra a continuación.
<table>
<tr><th>Máscara de subred</th><th>Dirección inicial de subred pública</th></tr>
<tr><td>255.255.0.0</td><td>Los últimos dos octetos deben terminar en 0.
EJEMPLO: 10.200.0.0</td></tr>
<tr><td>255.255.255.0</td><td>El último octeto debe terminar en 0.
EJEMPLO: 10.200.1.0.</td></tr>
<tr><td>255.255.255.128</td><td>El último octeto debe terminar en 0 o 128.
EJEMPLO: 10.200.1.0 o 10.200.1.128</td></tr>
<tr><td>255.255.255.192</td><td>El último octeto debe terminar en uno de los siguientes: 0, 64, 128, 192.
EJEMPLO: 10.200.1.64</td></tr>
<tr><td>255.255.255.224</td><td>El último octeto debe terminar en uno de los siguientes: 0, 32, 64, 96, 128, 160, 192, 224.
EJEMPLO: 10.200.1.32</td></tr>
<tr><td>255.255.255.240</td><td>El último octeto debe terminar en uno de los siguientes: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240.
EJEMPLO: 10.200.1.16</td></tr>
</table></td></tr>
<tr><td>Private IP Address</td><td>Escriba una dirección IP privada:
• Para traducir una sola dirección, escriba una dirección privada única que represente el dispositivo.
• Para traducir un rango de direcciones, escriba la primera dirección del rango de direcciones consecutivas.
• Para traducir direcciones en una subred, escriba una dirección inicial privada única que represente los dispositivos. Esta dirección debe corresponder al tamaño de la máscara de subred que se desea traducir tal como se muestra a continuación.
<table>
<tr><th>Máscara de subred</th><th>Dirección inicial de subred privada</th></tr>
<tr><td>255.255.0.0</td><td>Los últimos dos octetos deben terminar en 0.
EJEMPLO: 192.168.0.0</td></tr>
<tr><td>255.255.255.0</td><td>El último octeto debe terminar en 0.
EJEMPLO: 192.168.1.0</td></tr>
<tr><td>255.255.255.128</td><td>El último octeto debe terminar en 0 o 128.
EJEMPLO: 192.168.1.0 o 192.168.1.128</td></tr>
<tr><td>255.255.255.192</td><td>El último octeto debe terminar en uno de los siguientes: 0, 64, 128, 192.
EJEMPLO: 192.168.1.64</td></tr>
<tr><td>255.255.255.224</td><td>El último octeto debe terminar en uno de los siguientes: 0, 32, 64, 96, 128, 160, 192, 224.
EJEMPLO: 192.168.1.32</td></tr>
<tr><td>255.255.255.240</td><td>El último octeto debe terminar en uno de los siguientes: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240.
EJEMPLO: 10.200.1.16</td></tr>
</table></td></tr>
<tr><td>Type</td><td>Elija uno de estos valores:
• Single: traduce una sola dirección.
• Range: traduce un rango de direcciones.
• Subnet: traduce todas las direcciones de la subred pública o una porción de la subred pública.</td></tr>
<tr><td>Range</td><td>Escriba el número de direcciones que desea traducir. Este campo solo estará disponible si se ha elegido Range en el campo Type.
Valores válidos: 1…128
Valor predeterminado = 1
IMPORTANTE: Cada dirección del rango cuenta como una entrada de traducción. El switch admite un máximo de 128 entradas de traducción.</td></tr>
<tr><td>Subnet Mask</td><td>Escriba la máscara de subred de las direcciones que desea traducir.
Valores válidos:
• Clase B: 255.255.0.0
• Clase C: 255.255.255.0
• Porción de clase C:
– 255.255.255.128 (proporciona 128 direcciones por entrada de traducción)
– 255.255.255.192 (proporciona 64 direcciones por entrada de traducción)
– 255.255.255.224 (proporciona 32 direcciones por entrada de traducción)
– 255.255.255.240 (proporciona 16 direcciones por entrada de traducción)</td></tr>
</table>

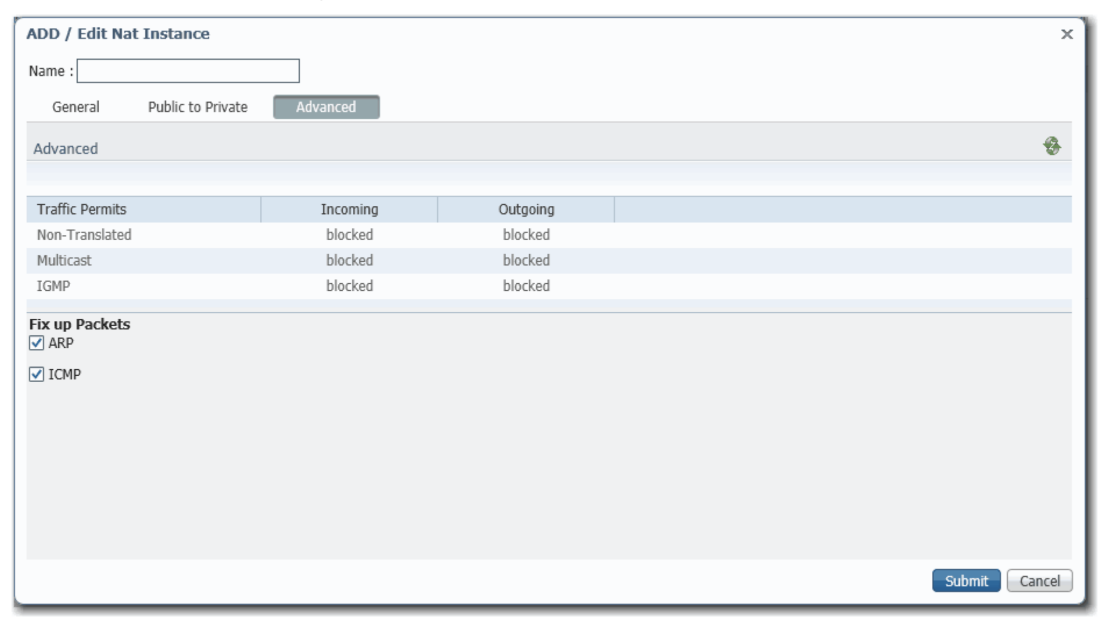
8. (Opcional). Si desea configurar permisos de tráfico y correcciones de paquetes, continúe con Configure permisos y correcciones de tráfico que aparece a continuación.
9. En la ventana NAT, haga clic en Submit.

Configure permisos y correcciones de tráfico

Tenga cuidado al configurar los permisos y las correcciones de tráfico. Le recomendamos que utilice los valores predeterminados.

Si desea configurar permisos o correcciones de tráfico, siga estos pasos.

1. Haga clic en la ficha Advanced.



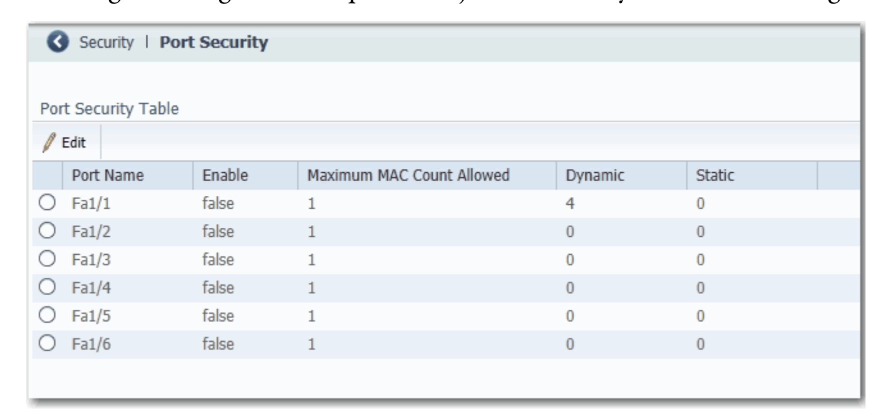
2. Elija una de estas opciones para los paquetes entrantes y salientes que no sean manejados por NAT:
   - Pass-through: permite que los paquetes atraviesen el límite de NAT.
   - Blocked: borra los paquetes.
3. En el área Fix up Packets, marque o desmarque las casillas de selección para habilitar o inhabilitar las correcciones para ARP e ICMP.

   De manera predeterminada, las correcciones están habilitadas para ARP e ICMP.
4. Haga clic en Submit.

Configure la seguridad de los puertos

Configure la seguridad de los puertos para limitar las direcciones MAC (ID MAC) que pueden obtener acceso a un determinado puerto. La seguridad del puerto se basa en el número de direcciones MAC admitidas (ninguna de las cuales se define de forma estática). La seguridad del puerto estática le permite especificar si las direcciones MAC se aprenden automáticamente o se definen manualmente.

Para configurar la seguridad del puerto, elija Port Security en el menú Configure.



La seguridad del puerto limita e identifica las direcciones MAC de los dispositivos que pueden enviar tráfico a través del puerto del switch. El puerto del switch no reenvía el tráfico procedente de dispositivos no incluidos en el grupo definido de dispositivos. Se produce una infracción de seguridad cuando se cumple cualquiera de las siguientes condiciones:

- Un dispositivo, que tiene una dirección MAC diferente de todas las direcciones MAC seguras identificadas, intenta obtener acceso al puerto del switch.
- El número de direcciones MAC del puerto supera el número máximo admitido en el puerto.

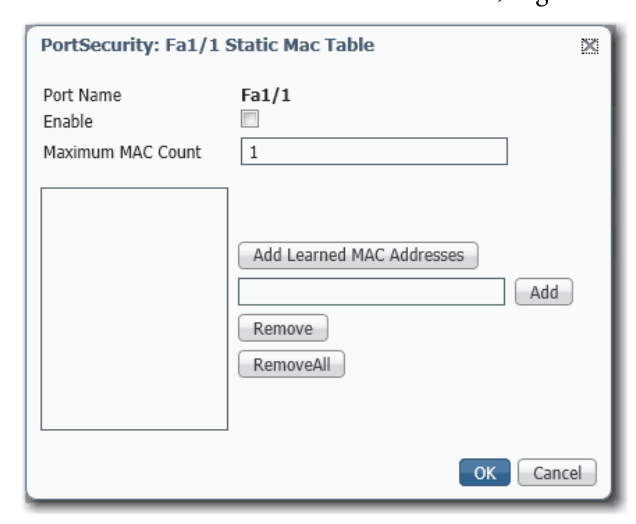
La seguridad del puerto admite varios niveles de seguridad:

- La capacidad de definir el número de dispositivos que se conectan a un determinado puerto. Estos se asignan por orden de llegada y caducan después de un determinado período de inactividad.
- La capacidad de almacenar fácilmente la configuración existente de direcciones MAC seleccionando Add Learned MAC Addresses en la tabla de direcciones MAC estáticas.
- La capacidad de añadir y eliminar manualmente direcciones MAC a nivel de cada puerto.

Para cambiar la tabla de direcciones MAC estáticas de un puerto, siga estos pasos:

1. Haga clic en el botón de radio situado junto al puerto que desea configurar.
2. Haga clic en Edit.
3. Desmarque o marque la casilla de verificación Enable.

4. Configure las direcciones MAC de la siguiente manera:
   - Para añadir las direcciones MAC existentes de los dispositivos conectados actualmente a un puerto, haga clic en Add Learned MAC Addresses.
   - Para añadir una determinada dirección MAC a la tabla, escriba una dirección MAC en los campos de formato y haga clic en Add.
   - Para eliminar una dirección MAC de la tabla, seleccione la dirección MAC y haga clic en Remove.
   - Para borrar la tabla de direcciones MAC, haga clic en Remove All.



5. Haga clic en OK.

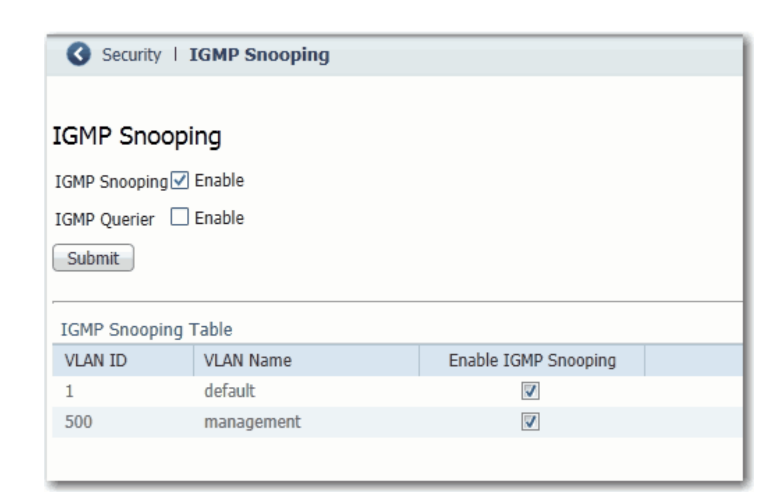
Configure IGMP Snooping

El IGMP (protocolo de administración de grupos de Internet) Snooping reduce el tráfico duplicado y en exceso de la red reenviando el tráfico de multidifusión IP a determinados puertos del switch en lugar de inundar todos los puertos.

Con IGMP Snooping, los puertos que solo son miembros de determinados grupos de multidifusión IP reciben mensajes de multidifusión. El resultado es un uso más eficiente del ancho de banda.

Para configurar IGMP Snooping, elija IGMP Snooping en el menú Configure:

- Para habilitar IGMP Snooping para todas las ID de VLAN, marque Enable junto a IGMP Snooping.
- Para habilitar IGMP Querier para todas las ID de VLAN, marque Enable junto a IGMP Querier.
- Para habilitar o inhabilitar IGMP Snooping en una VLAN, seleccione la VLAN y marque o desmarque la casilla de verificación Enable IGMP Snooping.

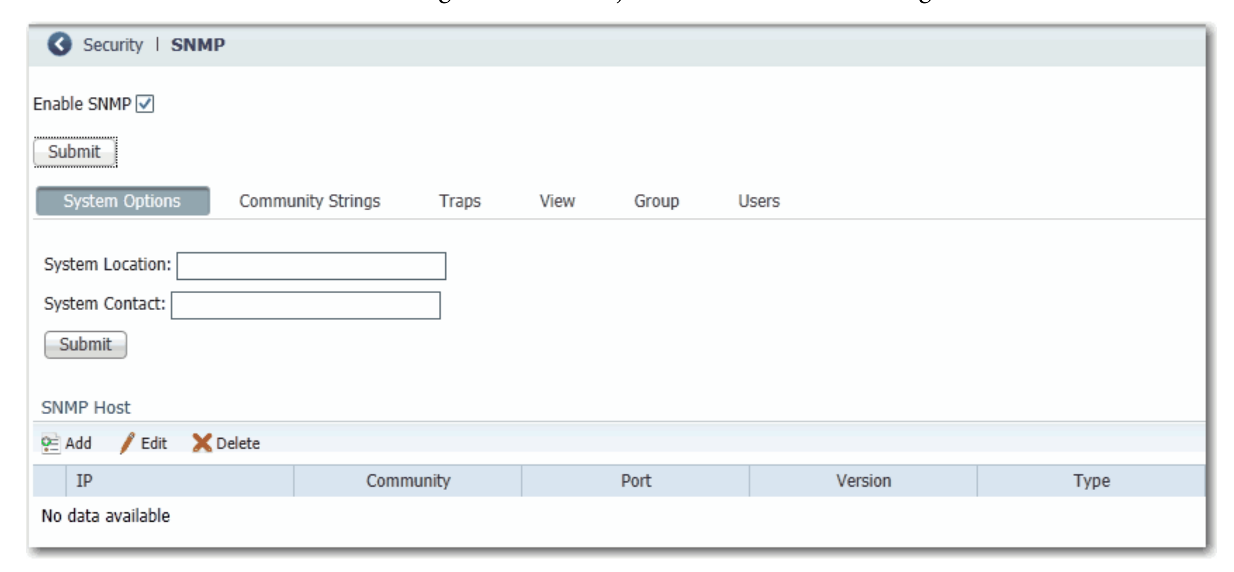


Configure SNMP

Habilite SNMP si tiene previsto administrar el switch a través de otra aplicación de administración de redes. De manera predeterminada, SNMP está inhabilitado.

Otros ajustes generales de SNMP incluyen el nombre del switch o el administrador de red y la ubicación del switch. El nombre del sistema y la información de contacto del sistema aparecen en el área Switch Information del Dashboard.

Para configurar SNMP, elija SNMP en el menú Configure.



Las cadenas de comunidad son contraseñas para la base de información de administración (MIB) del switch. Puede crear cadenas de comunidad que proporcionen a un administrador remoto acceso de solo lectura o acceso de lectura y escritura al switch.

Para crear, modificar y eliminar cadenas de comunidad, haga clic en la ficha Community Strings.



Una cadena de comunidad de solo lectura permite que el switch valide peticiones Get (solo lectura) provenientes de una estación de administración de redes. Si define la comunidad de lectura de SNMP, los usuarios podrán obtener acceso a los objetos MIB, pero no podrán cambiarlos.

Una cadena de comunidad de lectura y escritura permite que el switch valide peticiones Set (lectura y escritura) provenientes de una estación de administración de redes.

Utilice aplicaciones de administración de SNMP

Puede utilizar aplicaciones de administración de SNMP como, por ejemplo, IntraVue o HP OpenView, para configurar y administrar el switch. Consulte SNMP en la página 89 para obtener más información.

Configure ajustes de alarmas

El software del switch monitorea las condiciones a nivel de cada puerto o de manera global. Si las condiciones no coinciden con los parámetros establecidos, se activa una alarma o un mensaje del sistema. De manera predeterminada, el switch envía los mensajes del sistema a un centro de registro. Puede configurar el switch para que envíe interrupciones de SNMP a un servidor de SNMP. Puede configurar también el switch para que active un dispositivo de alarma externo utilizando los dos relés de alarma independientes.

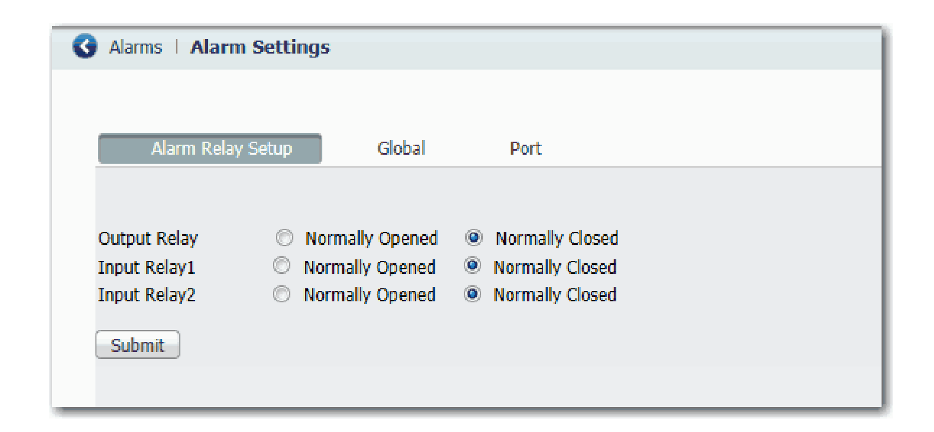
Ajustes de los relés de alarma

Puede configurar el switch para que active un dispositivo de alarma externo. El switch admite dos entradas de alarma y una salida de alarma. El software del switch está configurado para detectar fallos que se utilizan para energizar la bobina del relé y cambiar el estado de ambos contactos del relé. Los contactos normalmente abiertos se cierran y los contactos normalmente cerrados se abren.

Para configurar los ajustes de los relés de alarma, elija Alarm Settings en el menú Configure.

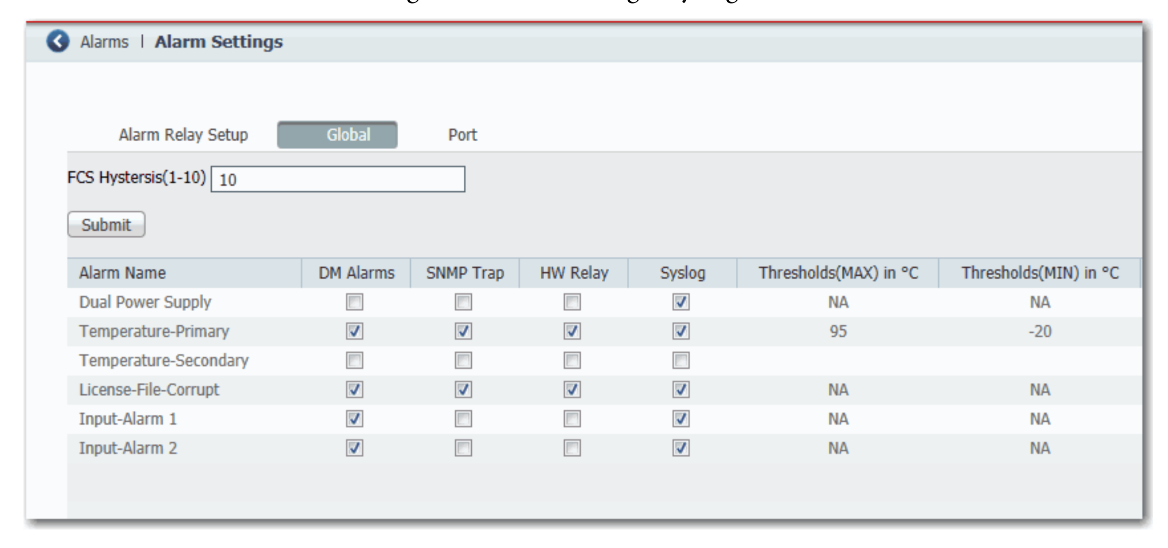
En la ficha Alarm Relay Setup, haga clic en una de estas opciones para cada tipo de relé de alarma:

- Normally Opened: la condición normal es que no fluye corriente a través de los contactos. Se genera la alarma cuando fluye corriente.
- Normally Closed: la condición normal es que fluya corriente a través de los contactos. Se genera la alarma cuando la corriente deja de fluir.



Alarmas globales

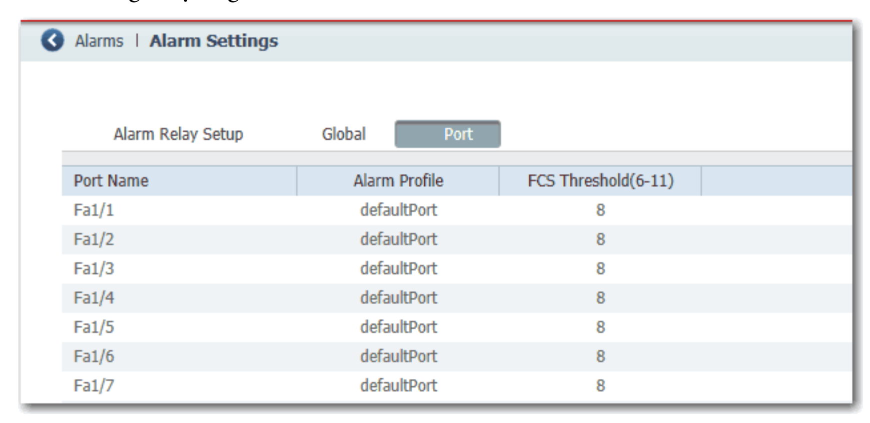
Para configurar alarmas globales, también denominadas alarmas del centro, elija Alarm Settings en el menú Configure y haga clic en la ficha Global.



Campo	Descripción
FCS Hysteresis (1-10)	El umbral de histéresis del error de secuencia de comprobación de trama (FCS) se utiliza para determinar cuando se borra una condición de alarma. Este valor se expresa como un porcentaje de la fluctuación de la proporción de errores de bits de FCS. El ajuste predeterminado es 8 por ciento. Puede ajustar el porcentaje para evitar que la condición se alarma se active y desactive cuando la proporción de errores de bits de FCS fluctúe cerca de la proporción de errores de bits configurada. Los porcentajes válidos para los ajustes globales son de 1 a 10. Este ajuste también se puede configurar en un puerto concreto con solo hacer clic en la ficha Port.
Alarm Name	Estos tipos de alarmas se pueden habilitar o inhabilitar: • Dual Power Supply: el switch monitorea los niveles de suministro de alimentación de CC. Si se ha configurado el sistema para que funcione en modo de alimentación doble, se activa una alarma si falla o falta una fuente de alimentación eléctrica. La alarma se borra automáticamente cuando las fuentes de alimentación están presentes o funcionan correctamente. Puede configurar la alarma de fuente de alimentación eléctrica para que esté conectada a los relés de hardware. • Temperature-Primary: estas alarmas se activan cuando la temperatura del sistema es superior o inferior a los umbrales configurados. De manera predeterminada, la alarma de temperatura primaria está asociada al relé principal. • Temperature-Secondary: estas alarmas se activan cuando la temperatura del sistema es superior o inferior a los umbrales configurados. • License-File-Corrupt: se activa una alarma cuando el archivo de licencia está alterado. • Input-Alarm 1: se activa una alarma en función de la alarma de entrada externa. • Input-Alarm 2: se activa una alarma en función de la alarma de entrada externa.
DM Alarms	La información de alarma aparece en el tablero de la interface web del administrador de dispositivos.
SNMP Trap	Las interrupciones de alarma se enviarán a un servidor de SNMP, si se ha habilitado SNMP en la ventana Configure > Security > SNMP.
HW Relay	Cuando se activa el relé de alarma del switch, envía una señal de fallo a un dispositivo de alarma externo conectado, como una campana, un indicador luminoso u otro dispositivo de señalización que haya configurado.
Syslog	Las interrupciones de alarma se registran en el syslog. Puede ver el syslog en la ventana Monitor > Syslog.
Thresholds (MAX) in °C	Umbral de temperatura máxima para la correspondiente alarma de temperatura primaria o secundaria, si se ha habilitado.
Thresholds (MIN) in °C	Umbral de temperatura mínima para la correspondiente alarma de temperatura primaria o secundaria, si se ha habilitado.

Alarmas de puertos

Para crear perfiles de alarma para puertos específicos, elija Alarm Settings en el menú Configure y haga clic en la ficha Port.



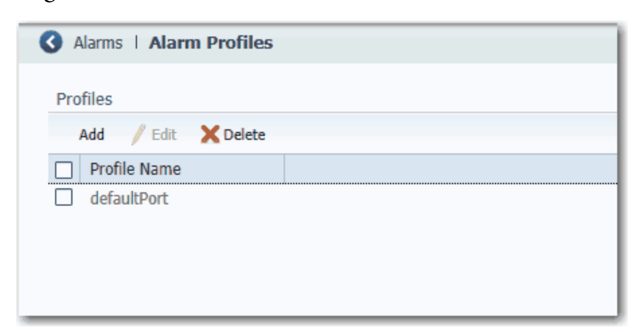
Para cada puerto, elija un perfil de alarma y defina el umbral FCS. El umbral de histéresis del error de secuencia de comprobación de trama (FCS) se expresa en forma de porcentaje de fluctuación de la proporción de errores de bits de FCS. El ajuste predeterminado es 8 por ciento. Puede ajustar el porcentaje para evitar que la condición se alarma se active y desactive cuando la proporción de errores de bits de FCS fluctúe cerca de la proporción de errores de bits configurada. Los porcentajes válidos para los ajustes de puerto son de 6 a 11.

Configure perfiles de alarmas

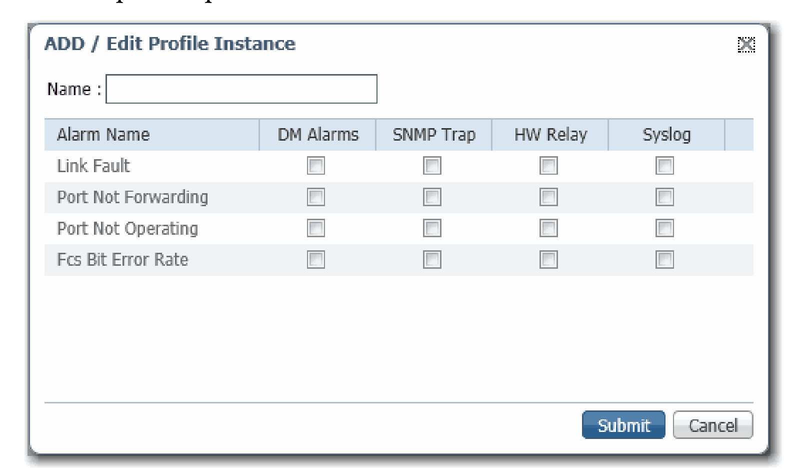
Puede utilizar perfiles de alarmas para aplicar un grupo de ajustes de alarmas a varias interfaces. Estos perfiles de alarmas se crean para que usted los use:

- defaultPort
- ab-alarm (se crea durante el proceso de configuración Express Setup)

Para crear, modificar y eliminar perfiles de alarmas, elija Alarm Profiles en el menú Configure.



En la ventana Add/Edit Profile Instance, puede configurar las alarmas y las acciones para un perfil de alarma.



Campo	Descripción
Name	Nombre único del perfil de alarma.
Alarm Name	Estos tipos de alarmas pueden activar una acción.
DM Alarms	La información de alarma aparece en el tablero de la interface web del administrador de dispositivos.
SNMP Trap	Las interrupciones de alarma se enviarán a un servidor de SNMP, si se ha habilitado SNMP en la ventana Configure > Security > SNMP.
HW Relay	Cuando se activa el relé de alarma del switch, envía una señal de fallo a un dispositivo de alarma externo conectado, como una campana, un indicador luminoso u otro dispositivo de señalización que haya configurado.
Syslog	Las interrupciones de alarma se registran en el syslog. Puede ver el syslog en la ventana Monitor > Syslog.

Monitoree tendencias

Puede ver datos históricos para que le ayuden a analizar los patrones de tráfico e identificar problemas. Los datos se pueden mostrar en incrementos de segundos, minutos, horas o días.

Para ver los datos en una tabla, haga clic en el botón Grid Mode que hay debajo del área. Para mostrar un gráfico, haga clic en el botón Chart Mode. Utilice los vínculos 60s, 1h, 1 d y 1 w para ver los datos en incrementos de 60 segundos, una hora, un día o una semana.

Para monitorear las tendencias, elija Trends en el menú Monitor.

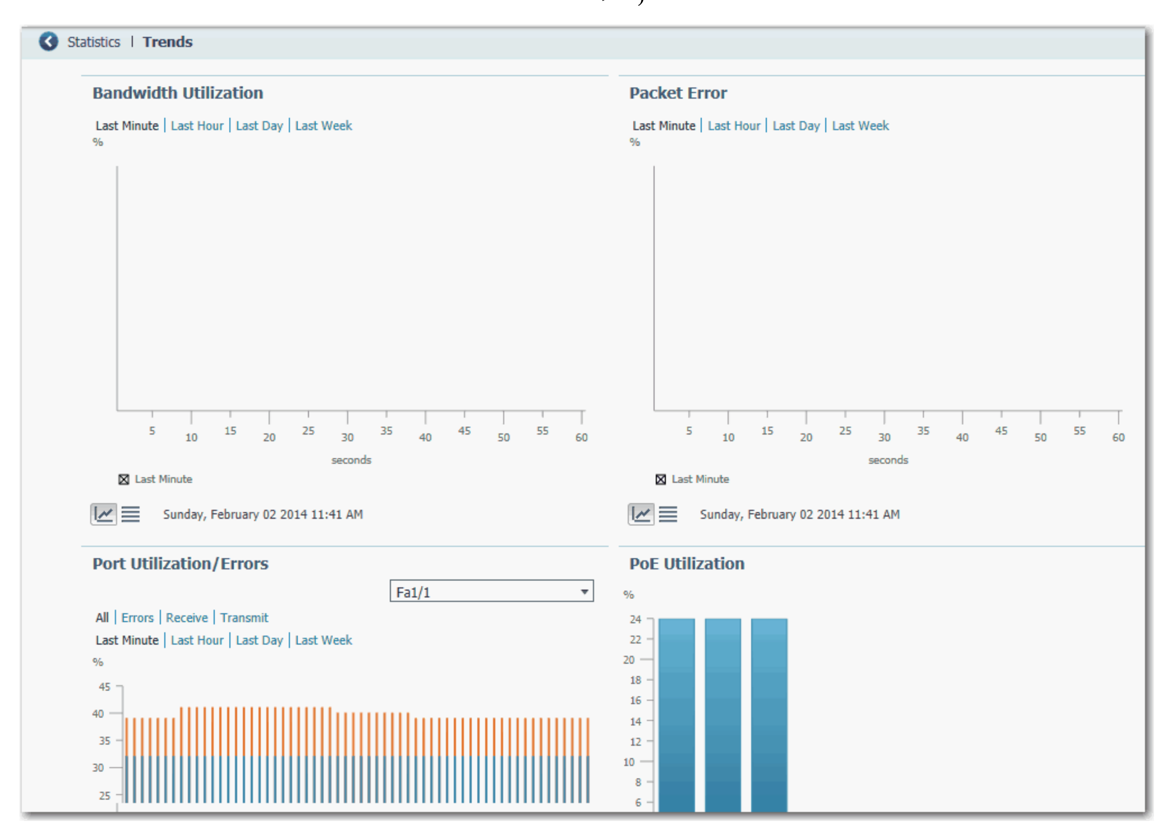


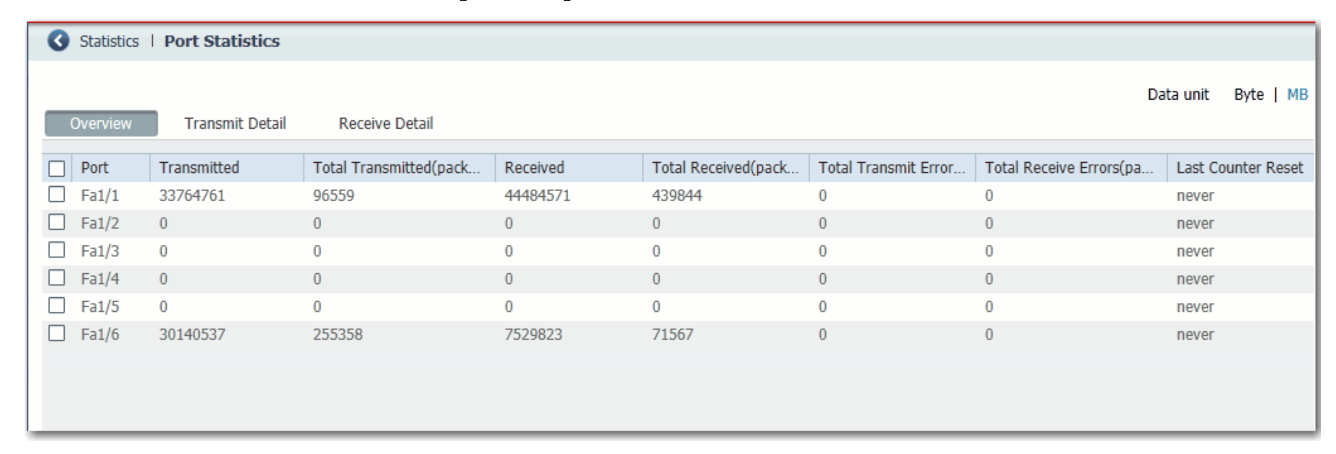
Tabla 17 - Gráficos de tendencias

Gráfico	Descripción
Bandwidth Utilization	El gráfico Bandwidth Utilization indica el porcentaje del ancho de banda disponible que se ha utilizado. El gráfico puede mostrar los patrones de uso del ancho de banda respecto a ocurrencias incrementales a lo largo del tiempo (por 60 segundos, 60 minutos, 24 horas o 14 días). En este gráfico también se marca el pico máximo alcanzado. El valor predeterminado es 60 segundos. Puede utilizar estos datos para determinar los momentos en los que la utilización de la red es alta o baja.
Packet Error	El gráfico Packet Error muestra el porcentaje de errores de paquetes recopilados respecto a ocurrencias incrementales a lo largo del tiempo (por 60 segundos, 60 minutos, 24 horas o 14 días). El valor predeterminado es 60 segundos. Utilice este gráfico para auditar los efectos que los dispositivos conectados tienen sobre el rendimiento del switch o sobre la red. Por ejemplo, si sospecha que un dispositivo conectado está enviando paquetes de errores, puede verificar si los datos del gráfico cambian al desconectar y volver a conectar el dispositivo sospechoso.
Port Utilization/Errors	El gráfico Port Utilization/Errors muestra los patrones de utilización de un determinado puerto respecto a ocurrencias incrementales a lo largo del tiempo (por 60 segundos, 60 minutos, 24 horas o 14 días). El valor predeterminado es 60 segundos. Para ver las tendencias correspondientes a un determinado puerto, elija un puerto de la lista Port. Utilice estos gráficos para observar el rendimiento de un determinado puerto. Por ejemplo, si un usuario de la red tiene conectividad de red intermitente, utilice el gráfico Port Utilization para observar los patrones de tráfico del puerto al que está conectada la computadora personal del usuario y emplee el gráfico Port Errors para ver si el puerto recibe o envía los paquetes de errores.
PoE Utilization	Para switches PoE, el gráfico PoE Utilization muestra la potencia asignada a los dispositivos conectados.

Monitoree estadísticas de puertos

Puede ver estadísticas relativas a los datos enviados y recibidos por los puertos del switch desde la última vez que se encendió o se reinició el switch, o desde que las estadísticas se borraron por última vez.

Para monitorear las estadísticas de los puertos, elija Port Statistics en el menú Monitor. Consulte la ayuda en línea de la interface web del administrador de dispositivos para obtener más información.



Port	Transmitted	Total Transmitted(pack...	Received	Total Received(pack...	Total Transmit Error...	Total Receive Errors(pa...	Last Counter Reset
Fa1/1	33764761	96559	44484571	439844	0	0	never
Fa1/2	0	0	0	0	0	0	never
Fa1/3	0	0	0	0	0	0	never
Fa1/4	0	0	0	0	0	0	never
Fa1/5	0	0	0	0	0	0	never
Fa1/6	30140537	255358	7529823	71567	0	0	never

Los tipos de estadísticas de puertos que se recopilan y muestran están agrupados en estas fichas en la ventana Port Statistics de la interface web del administrador de dispositivos:

- Ficha Overview: utilice esta ficha para ver los números específicos de paquetes de errores recibidos por el puerto o enviados desde el puerto, lo que constituye un nivel de detalle que no está disponible en los gráficos del tablero.

  El número de paquetes de errores puede corresponder a una desigualdad de modo dúplex, incompatibilidades con el puerto y su dispositivo conectado, o dispositivos conectados o cables defectuosos. Cualquiera de estos problemas puede ocasionar un bajo rendimiento de la red, pérdida de datos o falta de conectividad.

- Ficha Transmit Detail: utilice esta ficha para resolver problemas relacionados con cambios inusuales del tráfico de la red. Esta ficha muestra estas estadísticas:

  – Paquetes de unidifusión, multidifusión y difusión enviados desde cada puerto
  – Estadísticas detalladas de errores enviados a cada puerto

  Si un puerto está enviando una cantidad inusualmente alta de tráfico (como paquetes de multidifusión o difusión), monitoree el dispositivo conectado para determinar si este patrón de tráfico es normal o podría ser un indicio de que hay un problema.

- Ficha Receive Detail: utilice esta ficha para resolver problemas relacionados con cambios inusuales del tráfico de la red. Esta ficha muestra estas estadísticas:

  – Paquetes de unidifusión, multidifusión y difusión recibidos en cada puerto
  – Estadísticas detalladas de los errores recibidos en cada puerto

  Si un puerto recibe una cantidad inusualmente alta de tráfico (como paquetes de multidifusión o difusión), monitoree el dispositivo conectado para determinar si este patrón de tráfico es normal para el dispositivo conectado o podría ser un indicio de que hay un problema.

Monitoree las estadísticas de NAT

Puede monitorear estos tipos de estadísticas de NAT:

- Estadísticas globales para todas las ocurrencias
- Estadísticas por ocurrencia
- Traducciones privadas detalladas por ocurrencia
- Traducciones públicas detalladas por ocurrencia

Para ver la ventana NAT Statistics, elija NAT Statistics en el menú Monitor.

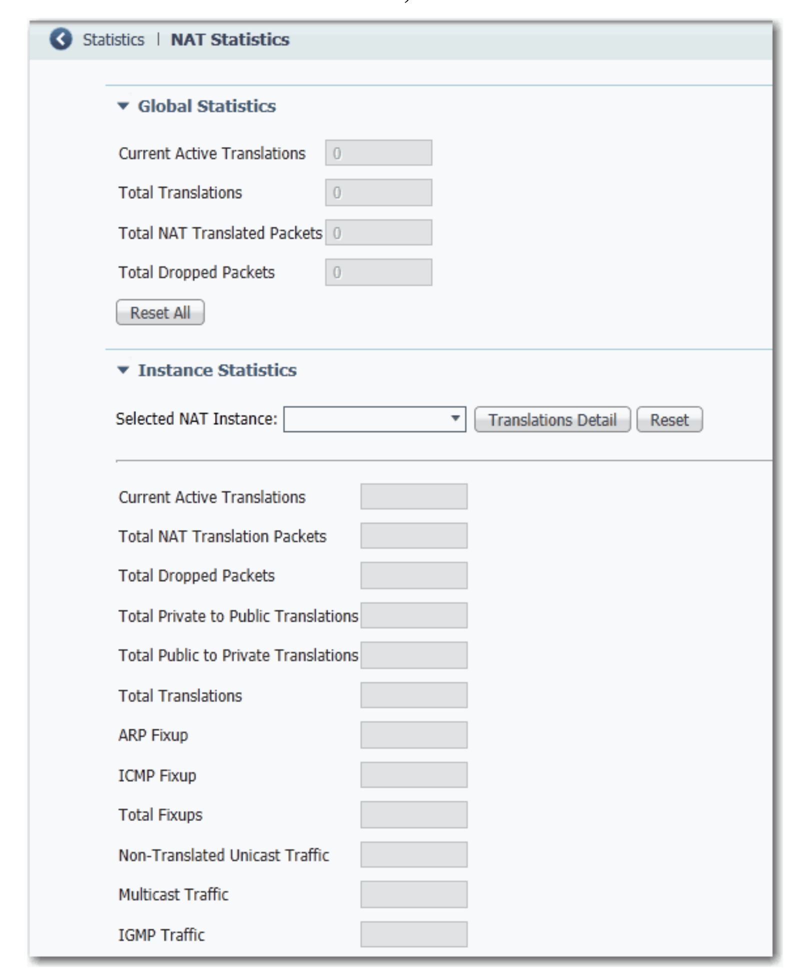


Tabla 18 - Estadísticas globales de NAT

Campo	Descripción
Current Active Translations	Número de direcciones IP que se han traducido en los últimos 90 segundos en todas las ocurrencias de NAT.
Total Translations	Número total de traducciones en todas las ocurrencias de NAT.
Total NAT Translated Packets	Número total de paquetes en todas las ocurrencias de NAT.
Total Dropped Packets	Número total de paquetes que se han eliminado en todas las ocurrencias de NAT.

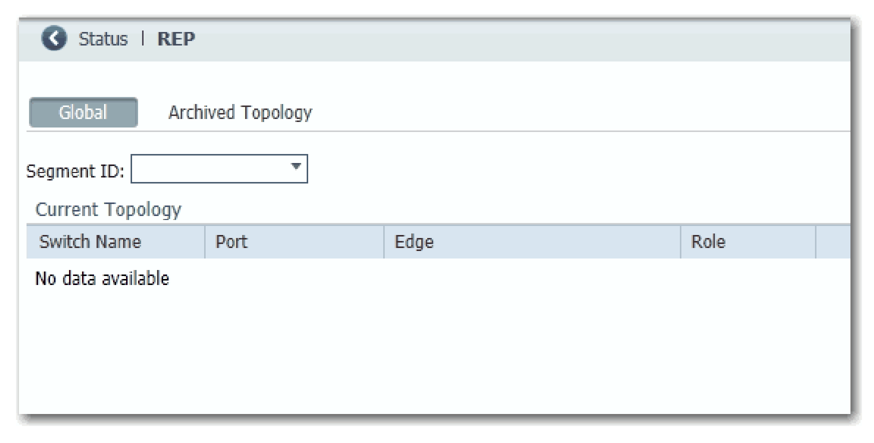
Tabla 19 - Estadísticas de ocurrencias

Campo	Descripción
Selected Instance	Elija en el menú desplegable la ocurrencia para la que desea ver las estadísticas.
Current Active Translations	Número de traducciones que se han realizado en los últimos 90 segundos para la ocurrencia.
Total NAT Translated Packets	Número total de paquetes que se han traducido para la ocurrencia.
Total Dropped Packets	Número total de paquetes que se han eliminado para la ocurrencia.
Total Private to Public Address Translations	Número total de traducciones configurado para los dispositivos de la subred privada.
Total Public to Private Address Translations	Número total de traducciones configurado para los dispositivos de la subred pública.
Total Translations	Número total de traducciones configurado para la ocurrencia.
ARP Fixup	Número de paquetes ARP que se han corregido para la ocurrencia.
ICMP Fixup	Número de paquetes ICMP que se han corregido para la ocurrencia.
Total Fixups	Número total de paquetes ARP e ICMP que se han corregido para la ocurrencia.
Non-Translated Unicast Traffic	Número de paquetes con tráfico de unidifusión no traducido para la ocurrencia.
Multicast Traffic	Número de paquetes con tráfico de multidifusión para la ocurrencia.
IGMP Traffic	Número de paquetes con tráfico IGMP para la ocurrencia.

Monitoree la topología del REP

Para revisar la topología del REP de uno o todos los segmentos de la red, elija REP en el menú Monitor.

Para mostrar una topología del REP archivada, haga clic en la ficha Archived Topology y seguidamente seleccione la ID del segmento.



Monitoree el estado de CIP

El protocolo industrial común (CIP) es un protocolo de mensajería de la capa de aplicación que utilizan diversos dispositivos de control y automatización industrial para comunicarse como parte de un sistema de control. CIP es la capa de aplicación de la red EtherNet/IP. Los switches Stratix contienen un servidor EtherNet/IP que permite que el switch forme parte de un sistema de control y automatización industrial para administración y monitoreo básicos.

La ventana CIP Status muestra información acerca del estado de CIP (campo Overview) y estadísticas (campo Request Details) desde la última vez que el switch se encendió o se reinició, o desde que los contadores se restablecieron la última vez.

Para resolver un problema, restablezca los contadores de CIP y vea si los contadores indican que el problema sigue existiendo.

IMPORTANTE	Excepto para los grupos de multidifusión activos, todas las demás categorías están relacionadas con el servidor CIP del switch, es decir, se refieren al tráfico de CIP dirigido específicamente al switch como dispositivo objetivo CIP. No se refieren al tráfico de CIP (EtherNet/IP) que fluye a través del switch entre los diversos controladores CIP, dispositivos HMI, herramientas de configuración y otros dispositivos objetivo CIP, como variadores, módulos de E/S, arrancadores de motores, sensores y válvulas.

Para monitorear el estado del CIP, elija CIP Status en el menú Monitor.

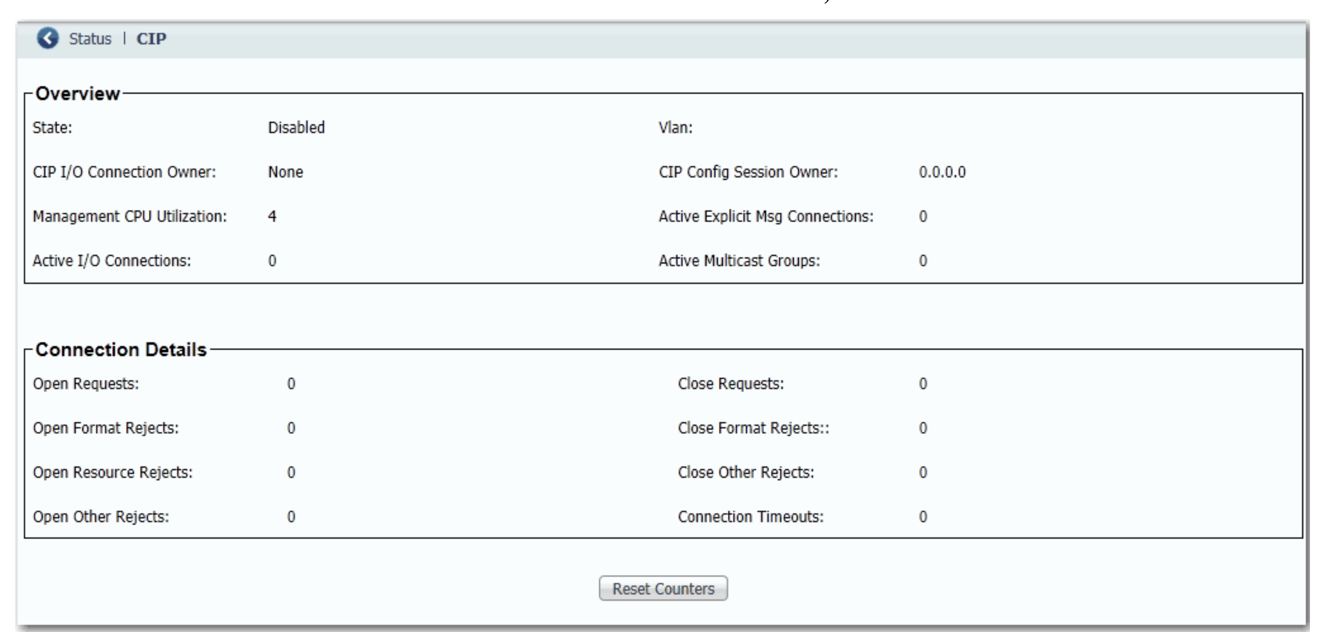


Tabla 20 - Campos de estado de CIP

Campo	Descripción
Overview	
State	Estado de la conexión CIP (habilitada o inhabilitada).
Vlan	ID de VLAN.
CIP I/O Connection Owner	Dirección IP del dispositivo al que se envían y desde el que se reciben datos de salida de E/S específicos de la aplicación.
CIP Config Session Owner	Dirección IP del dispositivo que controla la sesión de configuración del CIP.
Management CPU Utilization (%)	Porcentaje de la CPU de administración que se utiliza para funciones de administración. Las funciones del switch tienen ASIC dedicados que no se ven afectados por las funciones de administración.
Active Explicit Msg Connections	Número de conexiones activas de mensajería explícita con el switch como objetivo.
Active I/O Connections	Número de conexiones activas de E/S con el switch como objetivo.
Active Multicast Groups	Número de grupos de multidifusión, incluidos los grupos de multidifusión CIP que fluyen a través del switch.
Connection Details	
Open Requests	Número de peticiones de apertura de reenvío recibidas por el switch para establecer una conexión con el switch.
Close Requests	Número de peticiones de cierre de reenvío recibidas por el switch después de haberse establecido correctamente una conexión con el switch.
Open Format Rejects	Número de peticiones de apertura de reenvío dirigidas al switch que fallaron porque la petición no tenía el formato correcto.
Close Format Rejects	Número de peticiones de cierre de reenvío dirigidas al switch que fallaron porque la petición no tenía el formato correcto.
Open Resource Rejects	Número de peticiones de apertura de reenvío que no consiguieron establecer una nueva conexión por motivos como, por ejemplo, memoria insuficiente.
Close Other Rejects	Número de peticiones de cierre de reenvío que fallaron por motivos como, por ejemplo, una codificación electrónica incompatible.
Open Other Rejects	Número de peticiones de apertura de reenvío que fallaron por motivos como, por ejemplo, una codificación electrónica incompatible.
Connection Timeouts	Número de conexiones del CIP que sobrepasaron el tiempo de espera por inactividad.

Diagnostique problemas de cableado

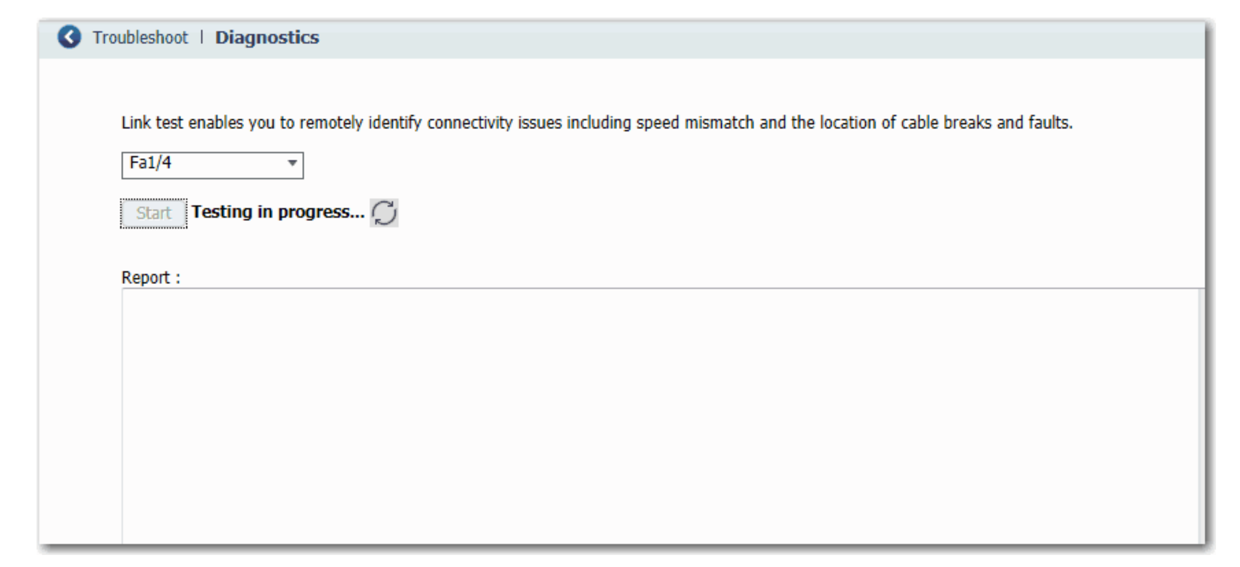
Utilice la ventana Diagnostics para ejecutar la prueba Broken Wire Detection, que utiliza la detección por reflectometría en el dominio del tiempo (TDR) para identificar, diagnosticar y resolver problemas de cableado. La detección por TDR es compatible con los puertos Ethernet 10/100 y 10/100/1000 de cobre. La TDR no es compatible con puertos de módulos enchufables con factor de forma pequeño (SFP).

La prueba de vínculo puede interrumpir el tráfico entre el puerto y el dispositivo conectado. Ejecute únicamente la prueba en un puerto donde sospeche que hay un problema. Antes de ejecutar la prueba de vínculo, utilice la vista del panel frontal y las ventanas Port Status y Port Statistics para recopilar información acerca de un posible problema.

IMPORTANTE	Para ejecutar una prueba válida en puertos gigabit, primero debe configurar el puerto gigabit como un tipo de medio físico RJ45, tal como se describe en Configure los ajustes de puerto en la página 109.

Para diagnosticar el cableado, elija Diagnostics en el menú Monitor.

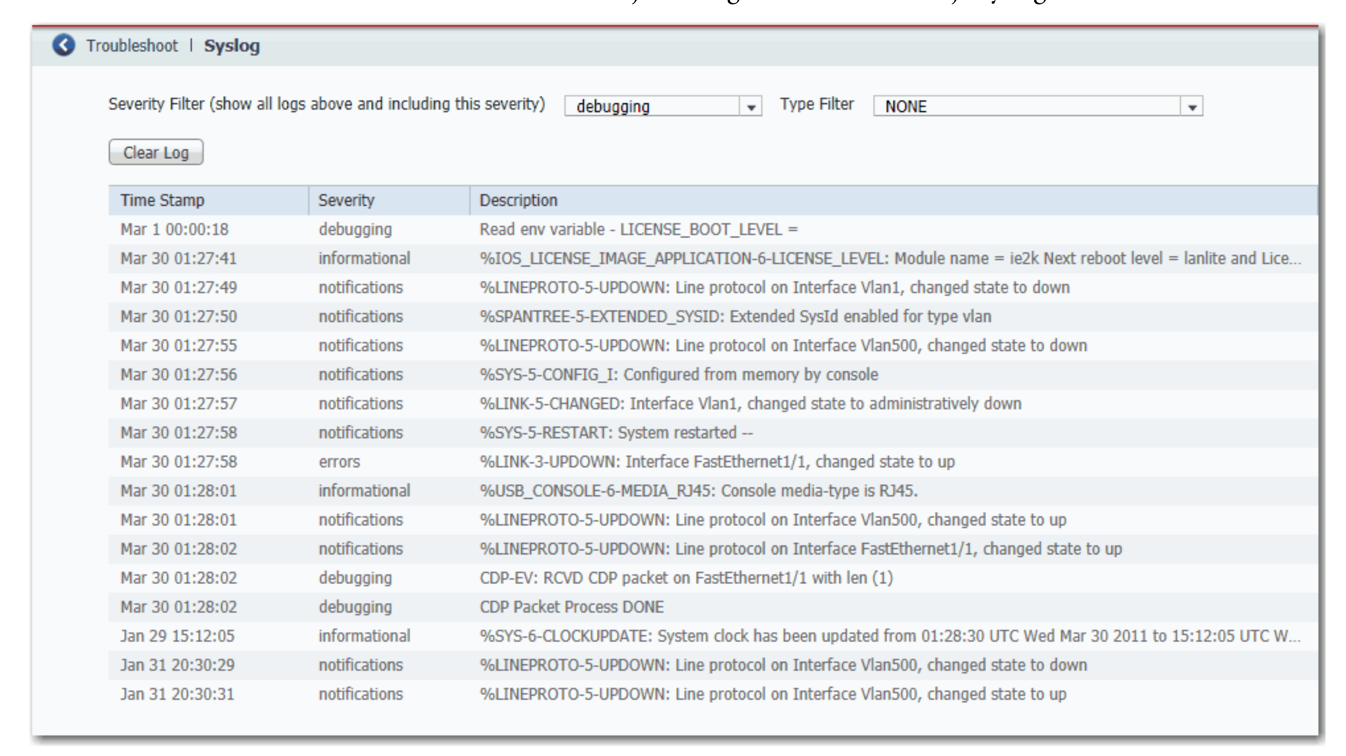
Para ejecutar una prueba, seleccione un puerto y haga clic en Start.



Vea mensajes de registro del sistema

El registro del sistema muestra los eventos que se han producido en el dispositivo y sus puertos, en función de los ajustes de alarma que haya configurado en la ventana Configure > Alarm Settings.

Para ver los mensajes del registro del sistema, elija Syslog en el menú Monitor.



Para filtrar eventos históricos, elija un filtro de gravedad o de tipo:

- Debugging: mensajes de depuración.
- Informational: mensajes informativos.
- Notifications: el switch funciona normalmente pero presenta una condición importante.
- Warnings: el switch presenta una condición de advertencia.
- Errors: el switch presenta una condición de error.
- Critical: el switch presenta una condición crítica.
- Alerts: el switch requiere una intervención inmediata.
- Emergencies: el switch no se puede utilizar.

Haga clic en Clear Log para confirmar que ha leído las alertas. Al hacer clic en Clear Log no se resuelve el problema.

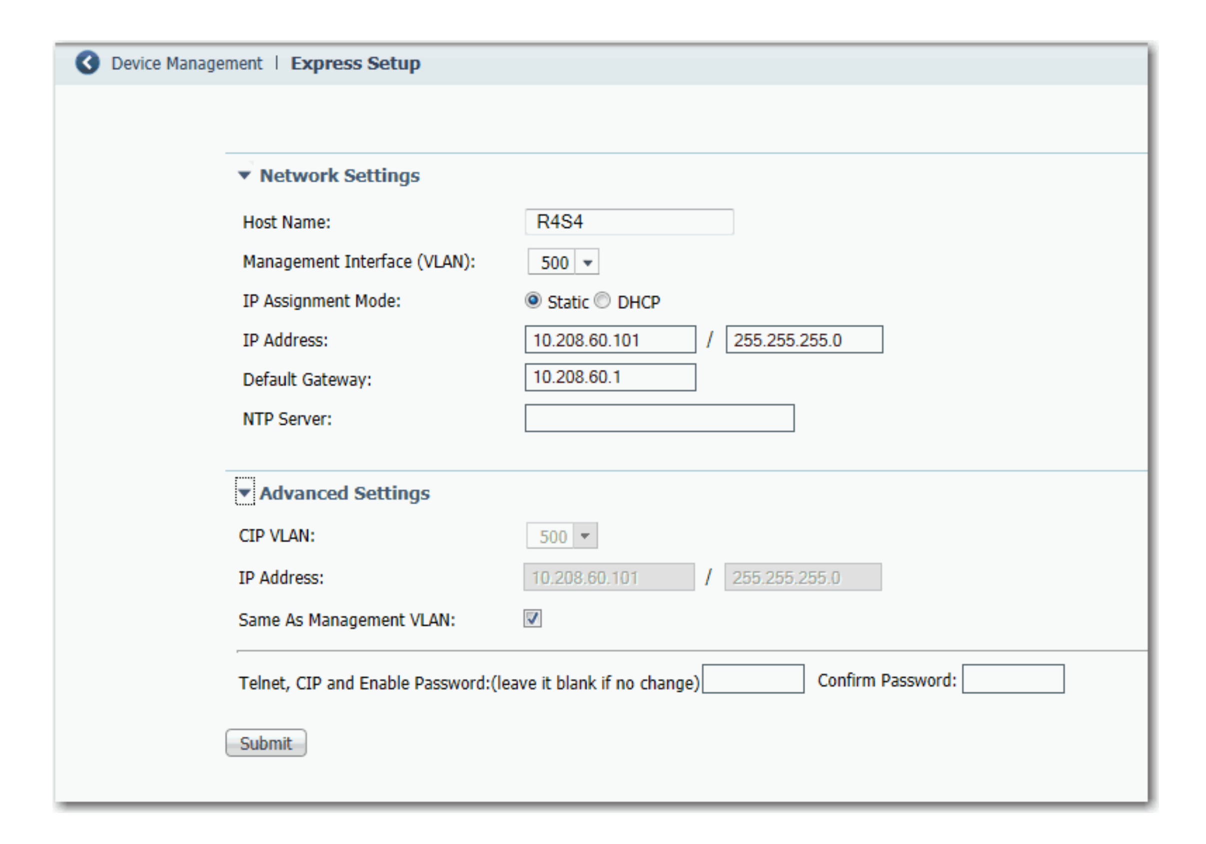
Tabla 21 - Campos de Syslog

Campo	Descripción
Time Stamp	Fecha y hora en la que se produjo el evento. Utilice la ventana Express Setup para conectar el dispositivo a un servidor NTP. Los ajustes de hora se perderán si el switch se queda sin alimentación.
Severity Level	Tipo y gravedad del evento.
Description	Descripción del problema, incluido el puerto en el que se detectó el problema.

Utilice Express Setup para cambiar los ajustes del switch

Los ajustes de red permiten que el switch funcione con sus ajustes predeterminados estándar y pueda administrarse mediante la interface web del administrador de dispositivos. Estos ajustes se definieron durante la configuración inicial. Cambie estos ajustes si desea trasladar el switch a una VLAN de administración diferente o a otra red.

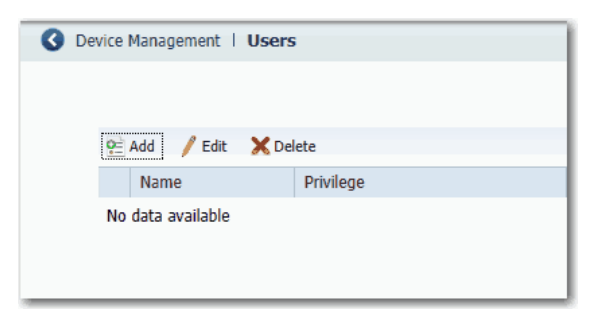
Para actualizar la información de IP del switch, elija Express Setup en el menú Admin.



Campo	Descripción
	Network Settings
Host Name	Nombre del dispositivo.
Management Interface (VLAN ID)	Nombre e ID de la VLAN de administración a través de la que se administra el switch. Elija una VLAN existente para que sea la VLAN de administración. La ID predeterminada es 1. El nombre predeterminado de la VLAN de administración es default. El número puede estar entre 1 y 1001. Asegúrese de que el switch y la estación de administración de red estén en la misma VLAN. De otra manera perderá la conectividad de administración con el switch. La VLAN de administración es el dominio de difusión a través del cual se envía el tráfico de administración entre determinados usuarios o dispositivos. Proporciona seguridad y control de difusión para el tráfico de administración que debe limitarse a un determinado grupo de usuarios como, por ejemplo, los administradores de su red. También proporciona acceso administrativo seguro a todos los dispositivos de la red en todo momento.
IP Assignment Mode	El modo de asignación de IP determina si la información de IP del switch se asigna manualmente (estática) o se asigna automáticamente mediante un servidor de protocolo de configuración dinámica de anfitrión (DHCP). El valor predeterminado es Static. Le recomendamos que haga clic en Static y asigne manualmente la dirección IP del switch. En lo sucesivo, podrá utilizar la misma dirección IP siempre que quiera obtener acceso a la interface web del administrador de dispositivos. Si hace clic en DHCP, el servidor DHCP asigna automáticamente una dirección IP, una máscara de subred y un gateway predeterminado al switch. Siempre que el switch no se reinicie, seguirá utilizando la información de IP asignada y usted podrá utilizar la misma dirección IP para obtener acceso a la interface web del administrador de dispositivos. Si asigna manualmente una dirección IP al switch y su red utiliza un servidor DHCP, asegúrese de que la dirección IP que especifique para el switch no esté dentro del rango de direcciones que el servidor DHCP asigna automáticamente a otros dispositivos. Así evitará conflictos de direcciones IP entre el switch y los demás dispositivos.
IP Address	La dirección IP y la máscara de subred asociada son identificadores únicos de un switch en una red: • El formato de dirección IP consiste en una dirección numérica de 32 bits escrita como cuatro números separados por puntos. Cada número puede estar entre 0 y 255. • La máscara de subred es la dirección de red que identifica la subred a la que pertenece el switch. Las subredes sirven para distribuir los dispositivos de una red en grupos más pequeños. La máscara predeterminada es 255.255.255.0. Este campo solo está habilitado si IP Assignment Mode está en Static. Asegúrese de que la dirección IP que asigne al switch no esté utilizada por ningún otro dispositivo de la red. La dirección IP y el gateway predeterminado no pueden ser iguales.
Default Gateway (opcional)	La dirección IP del gateway predeterminado. Un gateway es un encaminador o un dispositivo de red dedicado que permite que el switch se comunique con dispositivos de otras redes o subredes. La dirección IP del gateway predeterminado debe formar parte de la misma subred que la dirección IP del switch. La dirección IP del switch y la dirección IP del gateway predeterminado no pueden ser iguales. Si todos sus dispositivos se encuentran en la misma red y no se utiliza un gateway predeterminado, no es necesario que especifique ninguna dirección IP en este campo. Este campo solo está habilitado si el modo de asignación de IP es Static. Debe especificar un gateway predeterminado si su estación de administración de red y el switch se encuentran en redes o subredes diferentes. De otra manera, el switch y la estación de administración de red no podrán comunicarse entre sí.
NTP Server	Dirección IP del servidor de protocolo de tiempo de red (NTP). El NTP es un protocolo de conexión en red para la sincronización de relojes entre sistemas de computadoras mediante redes de datos de conmutación de paquetes de latencia variable.
	Advanced Settings
CIP VLAN	La VLAN en la que está habilitado el protocolo industrial común (CIP). La VLAN de CIP debe ser la misma que la VLAN de administración o se puede aislar el tráfico de CIP en otra VLAN que ya se haya configurado en este dispositivo.
IP Address	Dirección IP y máscara de subred de la VLAN de CIP si la VLAN de CIP es diferente de la VLAN de administración. El formato consiste en una dirección numérica de 32 bits escrita como cuatro números separados por puntos. Cada número puede estar entre 0 y 255. Asegúrese de que la dirección IP que asigne a este dispositivo no se utilice para ningún otro dispositivo de la red.
Same As Management VLAN	Indica si los ajustes de la VLAN de CIP son los mismos que los de la VLAN de administración.
Telnet, CIP and Enable Password (opcional)	Contraseña utilizada para la seguridad CIP y Telnet.
Confirm Password	La misma contraseña anterior.

Administre usuarios

Para añadir, modificar o eliminar usuarios e información de inicio de sesión del switch, elija Users en el menú Admin.



Para cada usuario, puede especificar la información en la siguiente tabla.

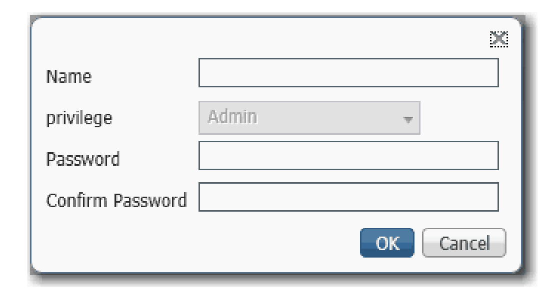


Tabla 22 - Campos para añadir usuarios

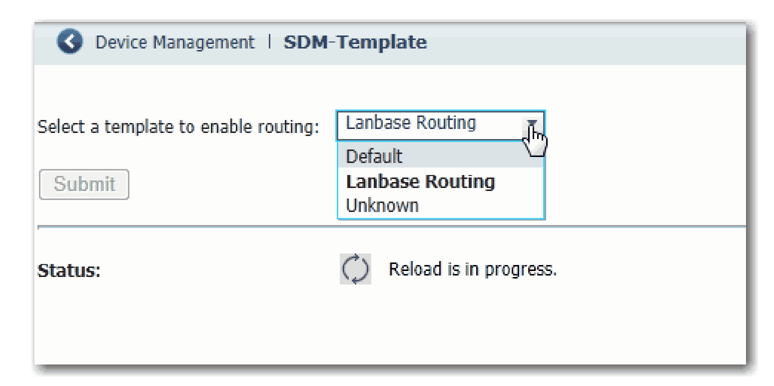
Campo	Descripción
Name	Nombre de usuario correspondiente a este usuario.
Privilege	Nivel de acceso de este usuario. A todos los usuarios se les asigna el privilegio Admin y pueden cambiar todos los parámetros.
Password	Contraseña necesaria para obtener acceso con este nombre de usuario.
Confirm Password	La misma contraseña anterior.

Reasigne memoria del switch para el encaminamiento

Las plantillas de base de datos de administración del switch (SDM) optimizan la forma en que se asigna la memoria del switch a determinadas características como, por ejemplo, el encaminamiento. Para habilitar el encaminamiento, debe cambiar la plantilla de SDM predeterminada a la plantilla Lanbase Routing.

Para aplicar una plantilla de SDM, siga estos pasos.

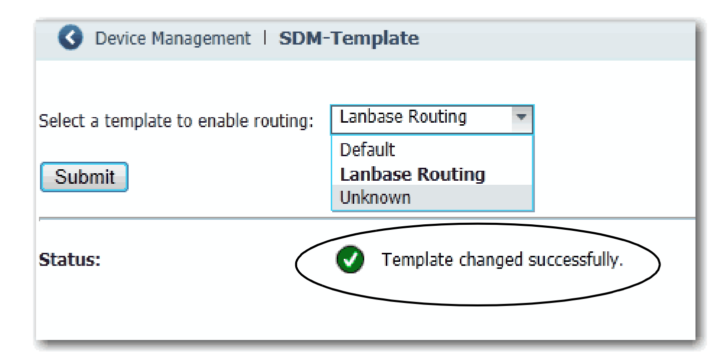
1. Elija SDM-Template en el menú Admin.
2. Seleccione una plantilla en el menú desplegable:
   - Default: equilibra todas las funciones de capa 2.
   - Lanbase Routing: maximiza los recursos del sistema para el encaminamiento de unidifusión IPv4, que se requiere para habilitar el encaminamiento.
   - Unknown: configurada por el usuario en la CLI.



3. Haga clic en Submit.
4. Cuando aparezca un mensaje que le pregunta si desea continuar, haga clic en OK.

IMPORTANTE	El proceso de cambio de la plantilla hace que el switch se reinicie automáticamente.

Aparecerá un mensaje una vez que el proceso haya finalizado.



5. Para habilitar el encaminamiento, continúe con Habilite y configure el encaminamiento en la página 124.

Reinicie el switch

Al reiniciar o restablecer el switch se interrumpe la conectividad de los dispositivos con la red.

Para reiniciar o restablecer el switch, elija Restart/Reset en el menú Admin.

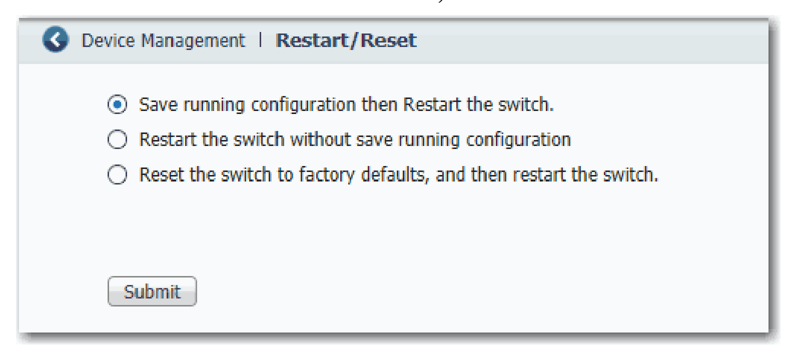


Tabla 23 - Campos para reiniciar/restablecer

Campo	Descripción
Save running configuration and then restart the switch	Garantiza que se guardan todos los cambios de la configuración de funcionamiento antes de reiniciar el switch.
Restart the switch without saving running configuration	Reinicia el switch con los ajustes de configuración anteriormente guardados.
Reset the switch to factory defaults, and then restart the switch	Restablece el dispositivo a los ajustes predeterminados establecidos en fábrica, para lo cual borra los ajustes de configuración actuales y seguidamente reinicia el dispositivo. Perderá la conectividad con el dispositivo y deberá iniciar Express Setup para volver a configurar el dispositivo.

Actualice el firmware del switch

Debe disponer de acceso a Internet para descargar el firmware del switch desde http://www.rockwellautomation.com a su computadora o unidad de red.

Para actualizar el switch con los cambios y las características del software más reciente, elija Software Update en el menú Admin.

Desde la interface web del administrador de dispositivos, puede actualizar los switches uno por uno.

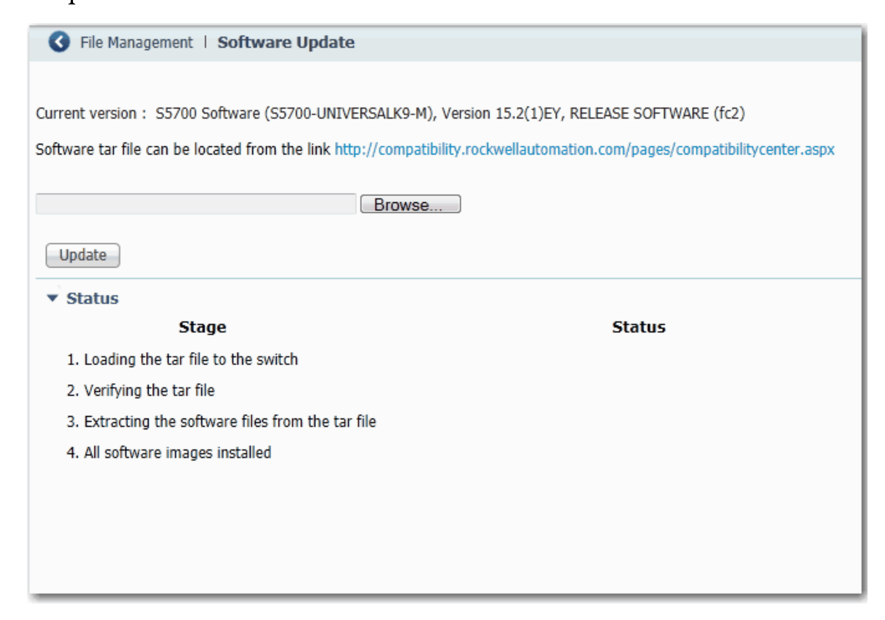
Con la revisión del firmware 2.001 o posterior, la actualización del firmware se instala en la ubicación de la memoria no volátil en ejecución:

- Si inicia el switch con la tarjeta SD insertada, la actualización se instala en la tarjeta SD.
- Si inicia el switch desde la memoria incorporada sin la tarjeta SD insertada, la actualización se instala en la memoria flash incorporada.

IMPORTANTE	Espere a que finalice el proceso de actualización. No utilice ni cierre la sesión del navegador en la que está activa la interface web del administrador de dispositivos. No intente obtener acceso a la interface web del administrador de dispositivos desde otra sesión de navegador.

Cuando termine el proceso de actualización, aparecerá un mensaje de finalización satisfactoria y el switch se reiniciará automáticamente. Es posible que el switch tarde unos minutos en reiniciarse con el nuevo firmware.

Compruebe que aparece la revisión del firmware más reciente del switch en el campo Software del área Switch Information del tablero.



Consulte la ayuda en línea de la interface web del administrador de dispositivos para conocer las pautas y procedimientos adicionales.

Utilice la tarjeta SD para sincronizar la configuración o los archivos IOS

Utilice la ventana Sync para sincronizar la tarjeta SD con la memoria incorporada. En la ficha Manual Sync, puede ver lo siguiente:

- Si se ha insertado una tarjeta
- Estado de la tarjeta
- Si se ha insertado, el origen desde el que se inició el switch

Puede sincronizar la configuración o el IOS de software, ya sea desde la tarjeta SD a la memoria incorporada, o bien desde la memoria incorporada a la tarjeta SD.

IMPORTANTE Puede sobrescribir la configuración si realiza la sincronización en la dirección incorrecta.

La ficha Auto Sync le permite configurar las opciones predeterminadas o la manera en que la interface web del administrador de dispositivos consulta al usuario después de un cambio de configuración o una actualización de IOS.

Para abrir esta ventana, elija Sync en el menú Admin.

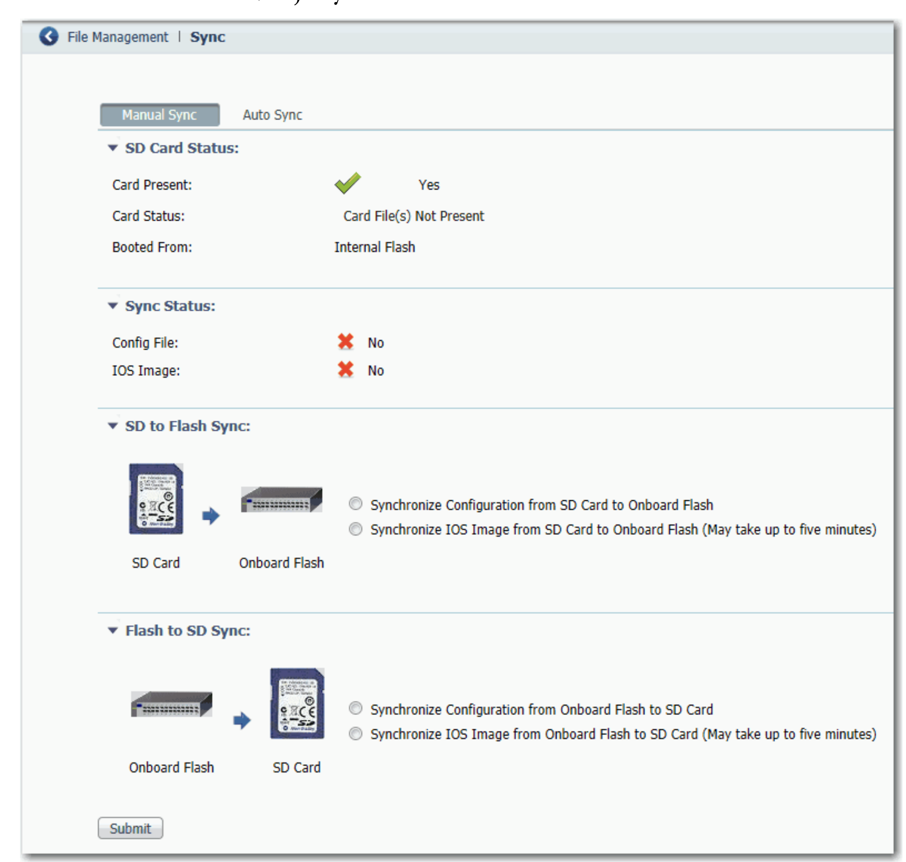


Tabla 24 - Campos de la ficha Manual Sync

Campo	Descripción
SD Card Status	Indica si se ha insertado una tarjeta SD, el estado de la tarjeta y desde dónde se inició su configuración.
SD to Flash Sync	Elija una de estas opciones: • Synchronize configuration from SD card to onboard flash • Synchronize IOS image from SD card to onboard flash
Flash to SD Sync	Elija una de estas opciones: • Synchronize configuration from onboard flash to SD card • Synchronize IOS image from onboard flash to SD card

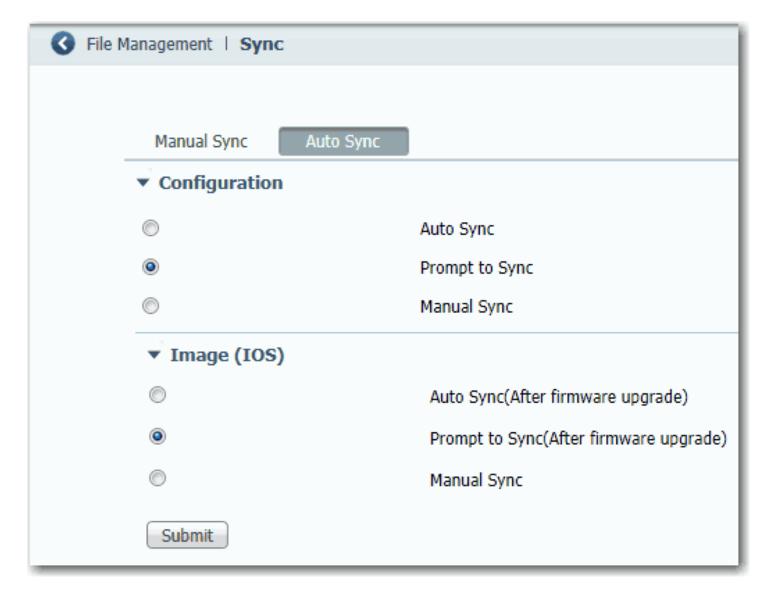


Tabla 25 - Campos de la ficha Auto Sync

Campo	Descripción
Configuration	Auto Sync: sincroniza automáticamente la configuración cuando se realiza un cambio de configuración en la interface web del administrador de dispositivos. Esta es la configuración predeterminada.
	Prompt to Sync: después de que un usuario haya enviado un cambio de configuración, se consulta al usuario con un mensaje que le solicita que confirme la sincronización.
	Manual Sync: no se realiza ninguna sincronización tras un cambio de configuración a menos que el usuario realice manualmente una sincronización.
Image (IOS)	Auto Sync (After firmware upgrade): sincroniza automáticamente la configuración cambiada cuando se actualiza el firmware.
	Prompt to Sync (After upgrade): tras actualizar el firmware, se consulta al usuario con un mensaje que le solicita que confirme la configuración. Esta es la configuración predeterminada.
	Manual Sync: no se realiza ninguna sincronización tras una actualización del firmware a menos que el usuario realice manualmente una sincronización.

Cargue y descargue archivos de configuración

Para copiar un archivo de configuración desde un archivo de otro dispositivo como, por ejemplo una PC, a la memoria incorporada, escriba el nombre de directorio de la carpeta del switch, navegue para seleccionar el archivo y haga clic en Upload.

Para descargar un archivo de configuración desde la memoria incorporada a su computadora, haga clic con el botón derecho del mouse en el vínculo y elija Save Link As.

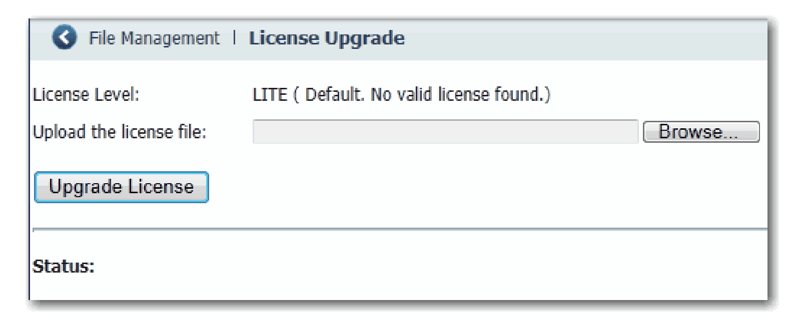


Actualice archivos de licencia

Tras obtener un archivo de licencia, utilice la ventana License Upgrade para instalarlo en el switch.

1. Haga clic en Browse para seleccionar el archivo de licencia.
2. Haga clic en Upgrade License para comenzar el proceso de actualización.

   Aparecerán mensajes de avance. Una vez finalizada la actualización, se reiniciará el switch.



Administración del switch mediante el ambiente Studio 5000

Tras finalizar el proceso de configuración Express Setup, puede administrar el switch mediante la aplicación Logix Designer en el ambiente Studio 5000.

Interface EtherNet/IP CIP

Los switches Stratix 5700 contienen una interface de redes de comunicación EtherNet/IP. La red EtherNet/IP es una especificación de red de automatización industrial que mantiene la asociación Open DeviceNet Vendor Association (ODVA). Utiliza el protocolo industrial común (CIP) para su capa de aplicación y TCP/UDP/IP para las capas de transporte y red. Es posible obtener acceso a esta interface mediante cualquiera de los puertos Ethernet del switch utilizando la dirección IP del switch.

Conexiones de red CIP

CIP es un protocolo basado en conexiones y orientado a objetos que admite dos tipos básicos de mensajería: conexiones explícitas e implícitas (E/S). Hay disponible un máximo de 32 conexiones. Ambos tipos de conexiones deben utilizar la contraseña del switch antes de que sea posible escribir cualquier parámetro del switch. La contraseña es la misma que especificó durante el proceso de configuración Express Setup.

Tabla 26 - Conexiones de red CIP

Conexión	Descripción
Mensajería explícita	Las conexiones de mensajería explícita proporcionan rutas de comunicación genéricas multiuso entre dos dispositivos. A estas conexiones con frecuencia se las denomina conexiones de mensajería. Los mensajes explícitos proporcionan una comunicación de red orientada a peticiones y respuestas. Normalmente, cada petición se dirige a un ítem de datos diferente. Los mensajes explícitos se pueden utilizar para configurar, monitorear y resolver los problemas del switch. La aplicación Logix Designer utiliza la interface de mensajería explícita.
E/S (mensajería implícita)	Las conexiones de E/S proporcionan rutas de comunicación dedicadas para fines especiales entre una aplicación que produce datos y una o varias aplicaciones que los consumen. Los datos de E/S específicos de la aplicación que se transfieren a través de estas conexiones suelen tener una estructura fija y cíclica. El switch admite dos opciones de conexión de E/S. • Solo entrada • Propietario exclusivo Ambas conexiones son cíclicas y pueden ajustarse entre 300 y 5000 ms. Una conexión de solo entrada contiene una estructura de datos con información de estado sobre el switch en general y el estado específico de cada uno de los puertos. Esta conexión es de multidifusión y puede ser compartida por varios controladores (originadores de conexión). Una conexión de propietario exclusivo utiliza la misma estructura de datos de entrada que una conexión de solo entrada, pero añade una estructura de datos de salida. Los datos de salida contienen un bit para cada puerto que le permite habilitar o inhabilitar cada puerto por separado. Mientras que varios controladores pueden compartir (mediante multidifusión) los datos de entrada de esta conexión, solo un controlador puede ser el propietario de los datos de salida. Si un segundo controlador intenta abrir esta conexión, se rechazará la conexión.

IMPORTANTE Dado que el controlador envía cíclicamente los datos de salida, se anulará cualquier otro intento de habilitar o inhabilitar un puerto realizado desde otra herramienta de software o estación de visualización.

Software RSLinx y compatibilidad con Network Who

La interface de redes EtherNet/IP también admite el comando List Identity que utilizan las herramientas de red basadas en CIP, como la función RSWho del software RSLinx®. RSWho le permite localizar e identificar su switch en la red mediante archivos de hojas electrónicas de datos (EDS).

Para obtener acceso a la función RSWho, en la barra de herramientas del software RSLinx, elija Communications > RSWho.

IMPORTANTE	Tras utilizar la función RSWho, si obtiene acceso al switch y consulta los contadores de vínculos Ethernet, verá únicamente los conteos correspondientes al primer puerto (puerto Gi1/1).

Archivos de hojas electrónicas de datos (EDS)

Los archivos de hojas electrónicas de datos (EDS) son archivos de texto simple que utilizan las herramientas de configuración de red como, por ejemplo, el software RSNetWorx™ for EtherNet/IP, para ayudarle a identificar los productos y ponerlos en marcha con facilidad en una red. Los archivos EDS contienen detalles acerca de los parámetros del dispositivo que se pueden leer y configurar. También le proporcionan información acerca de las conexiones de E/S que admite el dispositivo y el contenido de las estructuras de datos asociadas.

Si utiliza el switch en un sistema que no tiene un controlador basado en Logix de Rockwell Automation para monitorear o controlar el switch, no podrá utilizar el AOP suministrado con los controladores Logix. Debe utilizar la información de los archivos EDS para configurar la conexión de E/S.

El servidor OPC que contiene el software RSLinx Classic también utiliza archivos EDS para proporcionarle una lista de parámetros al añadir ítems (tags de OPC) a un tema (el switch).

Los archivos EDS de los switches Stratix 5700 se incluyen con los siguientes paquetes de software:

- Software RSLinx, versión 2.54 o posterior
- Software RSLogix 5000, versión 16 o posterior, o la aplicación Logix Designer, versión 21.00.00 o posterior
- Software RSNetWorx for EtherNet/IP, versión 9.0 o posterior

También puede obtener los archivos EDS mediante cualquiera de estas dos maneras:

- Desde http://www.rockwellautomation.com/resources/eds/.

  SUGERENCIA Para localizar un archivo EDS específico, haga lo siguiente:
  - Elija EtherNet/IP en el campo Network type.
  - Escriba Stratix 5700 en el campo Keyword.
  - Deje las entradas predeterminadas en los demás campos.

- Desde el switch, mediante la herramienta de instalación de hardware EDS de RSLinx.

Para cargar los archivos EDS directamente desde el switch a través de la red, siga estos pasos.

1. En el menú Start (Inicio), elija Programs (Programas) > Rockwell Software > RSLinx > Tools > EDS Hardware Installation Tool.
2. Haga clic en Add para abrir el asistente de EDS y añada la descripción de hardware seleccionada y los archivos asociados.

Datos accesibles con el CIP

La interface del CIP le permite obtener acceso a la siguiente información:

- Datos de entrada mediante conexión de E/S

  –Estado de vínculo por puerto: no conectado, conectado
  –Dispositivo no autorizado por puerto: correcto, incorrecto
  –Umbral de unidifusión excedido por puerto: correcto, excedido
  –Umbral de multidifusión excedido en cada puerto: correcto, excedido
  –Umbral de difusión excedido en cada puerto: correcto, excedido
  –Utilización de ancho de banda de puerto, por puerto: valor en %
  –Relé principal de alarma: correcto, activado
  –Grupos de multidifusión activos: cantidad

- Datos de salida mediante conexión de E/S

  –Inhabilitación de puerto, por puerto: habilitado, inhabilitado

- Otros datos de estado

  – Temperatura interna del switch: grados centígrados
  – Fuente de alimentación eléctrica A presente: sí, no
  – Fuente de alimentación eléctrica B presente: sí, no
  – Información de identidad: ID de proveedor, tipo de dispositivo, código de producto, nombre de producto, revisión, número de serie
  – Versión de lanzamiento de IOS
  – Tiempo de actividad del switch desde el último reinicio
  – Utilización de la CPU de administración: en porcentaje
  – Contadores de conexiones del CIP: peticiones de apertura/cierre, rechazos de apertura/cierre, tiempos de espera excedidos
  – Estado de alarma de puerto, por puerto: correcto, sin reenvío, no operativo, errores de FCS excesivos
  – Estado de fallo de puerto, por puerto: inhabilitación por error, error de SFP, desigualdad de VLAN nativa, condición MAC Address Flap, infracción de seguridad
  – Contadores de diagnóstico de puerto, por puerto: contadores de interface Ethernet (10), contadores de medios Ethernet (12)

- Datos de configuración (requiere contraseña)
  - Método de dirección IP: DHCP, estático
  - Dirección IP, máscara de subred, gateway predeterminado (todos si es estático)
  - Nombre de anfitrión
  - Nombre de contacto
  - Ubicación geográfica
  - Configuración de puerto, por puerto: habilitar/inhabilitar, autonegociar, velocidad/dúplex forzados
  - ID MAC autorizada por puerto
  - Umbral límite de velocidad de unidifusión por puerto: en paquetes por segundo, bits por segundo o porcentaje
  - Umbral límite de velocidad de multidifusión: en paquetes por segundo, bits por segundo o porcentaje
  - Umbral límite de velocidad de difusión: en paquetes por segundo, bits por segundo o porcentaje
- Asignación de Smartport por puerto: rol y VLAN
- Guardar y restaurar la configuración del switch (mediante File Obj)

Añadir un switch al árbol de configuración de E/S

Para añadir el switch al árbol de E/S del controlador, siga estos pasos.

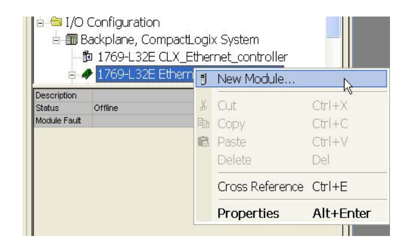
IMPORTANTE	Es necesario que realice estos pasos antes de poder entrar en línea para configurar y monitorear el switch.

1. Abra el archivo de proyecto correspondiente al controlador que monitorea el switch.
2. Seleccione el módulo de Ethernet mediante el cual el controlador se comunica con el switch.

   En este ejemplo, el switch se comunica mediante un controlador 1769-L32E CompactLogix EtherNet/IP.



3. Haga clic con el botón derecho del mouse en el puerto Ethernet que ha creado y elija New Module.



4. Haga clic en Communications.

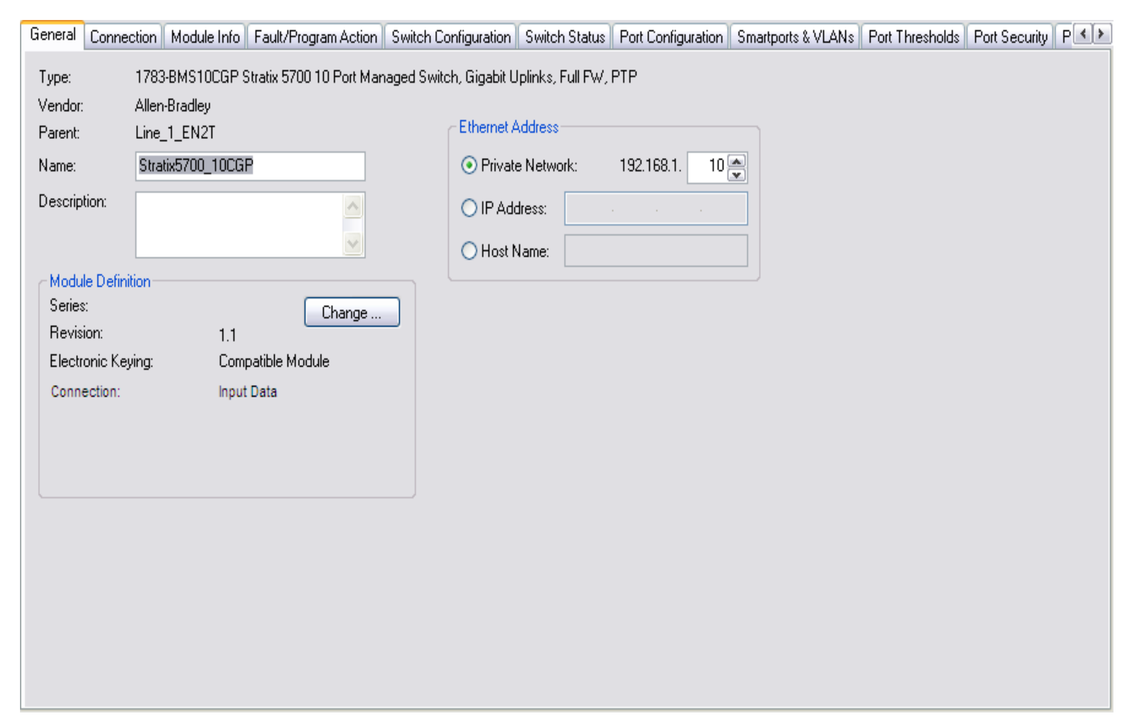
5. Haga clic en el signo + y baje hasta que vea el switch que desea configurar.

   Si el switch no aparece en la lista, puede obtener el AOP en el sitio web del servicio de asistencia técnica de Rockwell Automation.

   a. Visite http://www.rockwellautomation.com/support/.
   b. Haga clic en Downloads/RSLogix 5000 I/O Modules Add-on Profiles.
   c. Elija 1783-Stratix 5700 Managed Switches Add-on Profile.

6. Haga clic en OK para ver el cuadro de diálogo Module Properties.

Configure propiedades generales



Para configurar las propiedades generales, siga estos pasos.

1. En el cuadro de diálogo Module Properties, rellene los campos que se describen a continuación.

Campo	Descripción
Name	Nombre elegido para el switch.
Description	Descripción que le ayude a recordar algo importante acerca del switch.
Ethernet Address	Elija una de las siguientes opciones: • Private Network: red privada en la que se encuentra el switch. • IP Address: dirección IP que especificó al realizar el proceso de configuración Express Setup. El controlador utiliza la dirección IP para comunicarse. • Host Name: nombre de anfitrión que indicó en la configuración inicial cuando realizó el proceso de configuración Express Setup. El nombre de anfitrión requiere que tenga un servidor DNS configurado en la red del módulo de interface Ethernet del controlador. **IMPORTANTE:** Asegúrese de que la dirección IP y el nombre de anfitrión sean los mismos que los que se indicaron al realizar el proceso de configuración Express Setup.

2. Haga clic en OK.
3. Entre en línea con el switch; para ello elija Communications > Go online.

4. Haga doble clic en el switch para ver el cuadro de diálogo Module Properties.
5. Haga clic en Change.
6. Rellene los campos del cuadro de diálogo Module Definition.



Campo	Descripción
Revision	Revisión mayor y menor del switch: • Revisión mayor: un número entre 1 y 128 • Revisión menor: un número entre 1 y 255
Electronic Keying	• Compatible Module (opción predeterminada) • Exact Match • Disable Keying
Connection	• Input Data (opción predeterminada): habilita solo la conexión de datos de entrada • Data: habilita la conexión de datos de entrada y salida **ATENCIÓN:** Esta selección habilita los tags de salida, que pueden inhabilitar puertos e interrumpir conexiones al switch y a través del mismo. Puede inhabilitar un puerto del switch, para lo cual debe establecer el bit correspondiente en el tag de salida. Los bits de salida se aplican cada vez que el switch recibe los datos de salida del controlador cuando el controlador está en modo de marcha. Cuando el controlador está en modo de programación, no se aplican los bits de salida. El puerto está habilitado si el correspondiente bit de salida es 0. Si habilita o inhabilita un puerto utilizando la interface web del administrador de dispositivos o la CLI, el ajuste del puerto se podrá anular mediante los bits de salida procedentes del controlador en la siguiente actualización cíclica de la conexión de E/S. Los bits de salida siempre tienen prioridad, independientemente de si se utilizó la interface web del administrador de dispositivos o la CLI para habilitar o inhabilitar el puerto.
Data Connection Password	Escriba la contraseña para obtener acceso al switch. Solo es necesaria para la conexión de datos.

Propiedades de conexión

Puede definir las propiedades de conexión del switch en la ficha Connection.

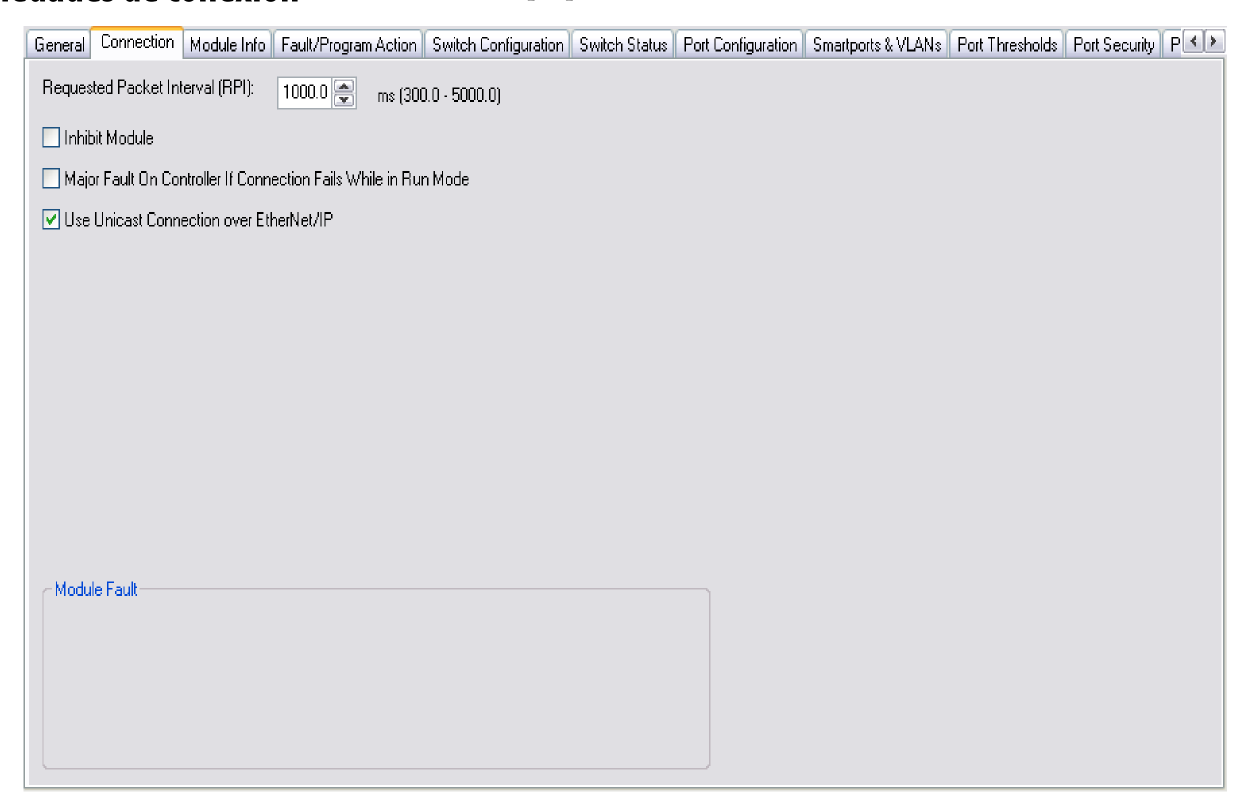


Tabla 27 - Campos de la ficha Connection

Campo	Descripción
Requested Packet Interval (RPI)	Escriba un valor entre 300 y 5000.
Inhibit Module	Marque la casilla para inhabilitar la comunicación entre el controlador y el switch. Desmarque la casilla para restaurar la comunicación.
Major Fault on Controller If Connection Fails While in Run mode	Marque esta casilla para que el controlador cree un fallo mayor si la conexión falla en modo de marcha.
Use Unicast Connections over EtherNet/IP	Marque esta casilla para utilizar conexiones de unidifusión con la red EtherNet/IP.
Module Fault	Muestra el código de fallo devuelto desde el controlador (relacionado con el switch que está configurando) y el texto que detalla el fallo de módulo que se ha producido.

Información del módulo

Puede monitorear y restablecer el switch desde la ficha Module Info.

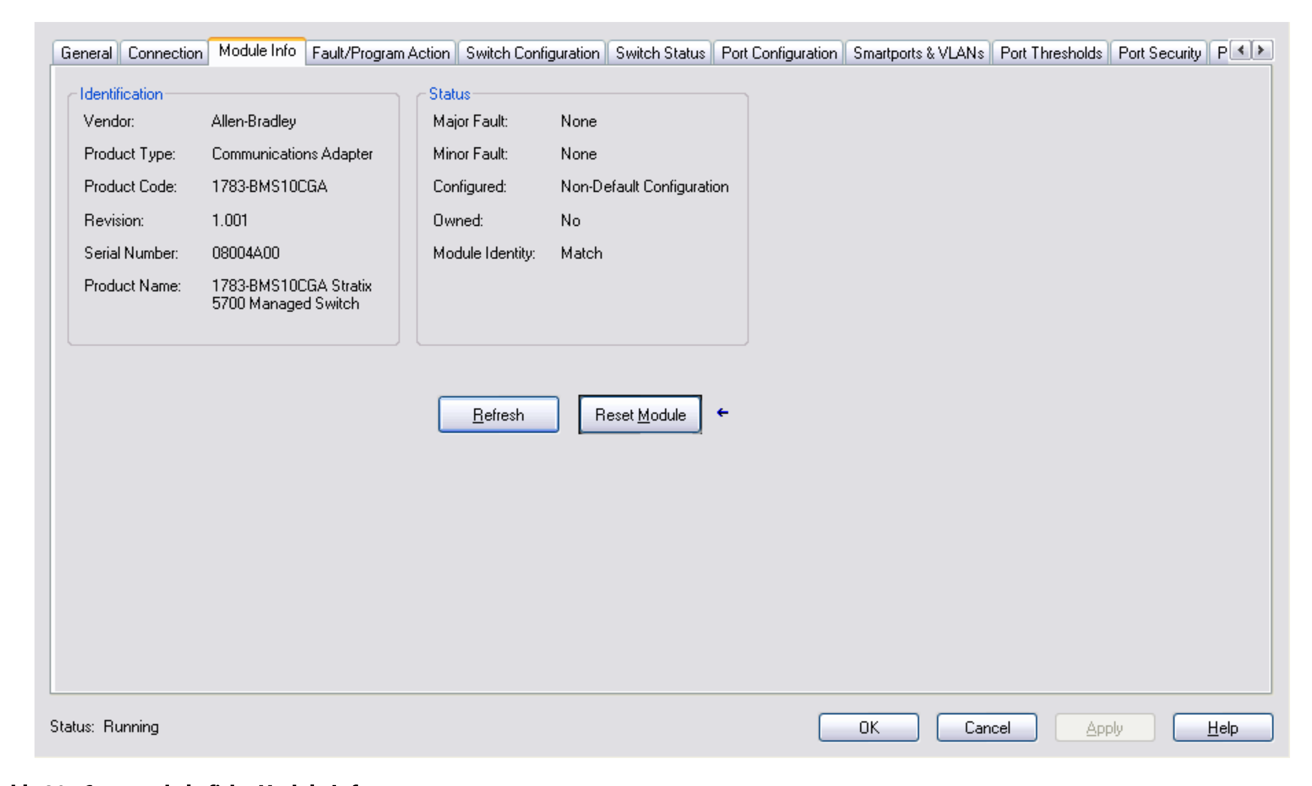


Tabla 28 - Campos de la ficha Module Info

Campo	Descripción
Identification	Muestra la siguiente información acerca del switch: • Proveedor • Tipo de producto • Código de producto • Revisión • Número de serie • Nombre de producto
Status	Muestra el estado de lo siguiente: • Estado de fallo mayor/menor: – Ninguno – Recuperable – No recuperable • Configuración: – Configuración diferente a la predeterminada – Configuración predeterminada • Con propietario. Indica si hay una conexión de E/S: – Sí – No • Identidad del módulo: – Coincide. Coincide con lo especificado en la ficha General. Para que exista esta condición de coincidencia, el proveedor, el tipo de producto, el código de producto y la revisión mayor deben coincidir. – No coincide. No coincide con lo especificado en la ficha General. El campo Module Identify no tiene en cuenta la selección de codificación electrónica o revisión menor del switch que se especificó en la ficha General.
Refresh	Haga clic para actualizar la ficha con nuevos datos provenientes del módulo.
Reset Module	Haga clic para restablecer el switch (desconectar y volver a conectar la alimentación eléctrica) con el archivo de configuración actual. Puede que aparezca el cuadro de diálogo Password Confirmation. **ATENCIÓN**: Al restablecer un módulo se cerrarán todas las conexiones que vayan al módulo o que lo atraviesen, lo que puede ocasionar una pérdida de control.

Propiedades de configuración del switch

Puede configurar los ajustes de IP y los parámetros administrativos desde la ficha Switch Configuration. Debe estar en línea para realizar esta configuración. En el modo fuera de línea, no aparecerá nada en esta ficha.

La dirección IP puede asignarse manualmente (estática) o automáticamente mediante un servidor de protocolo de configuración dinámica de anfitrión (DHCP). El valor predeterminado es Static. Le recomendamos que elija Static y asigne manualmente la dirección IP del switch. A continuación, puede utilizar la misma dirección IP siempre que quiera obtener acceso al switch.

- Static: escriba manualmente la dirección IP, la máscara de subred y el gateway.
- DHCP: el switch obtiene automáticamente una dirección IP, el gateway predeterminado y la máscara de subred del servidor DHCP. Siempre que no se reinicie el switch, seguirá utilizando la información de IP asignada.

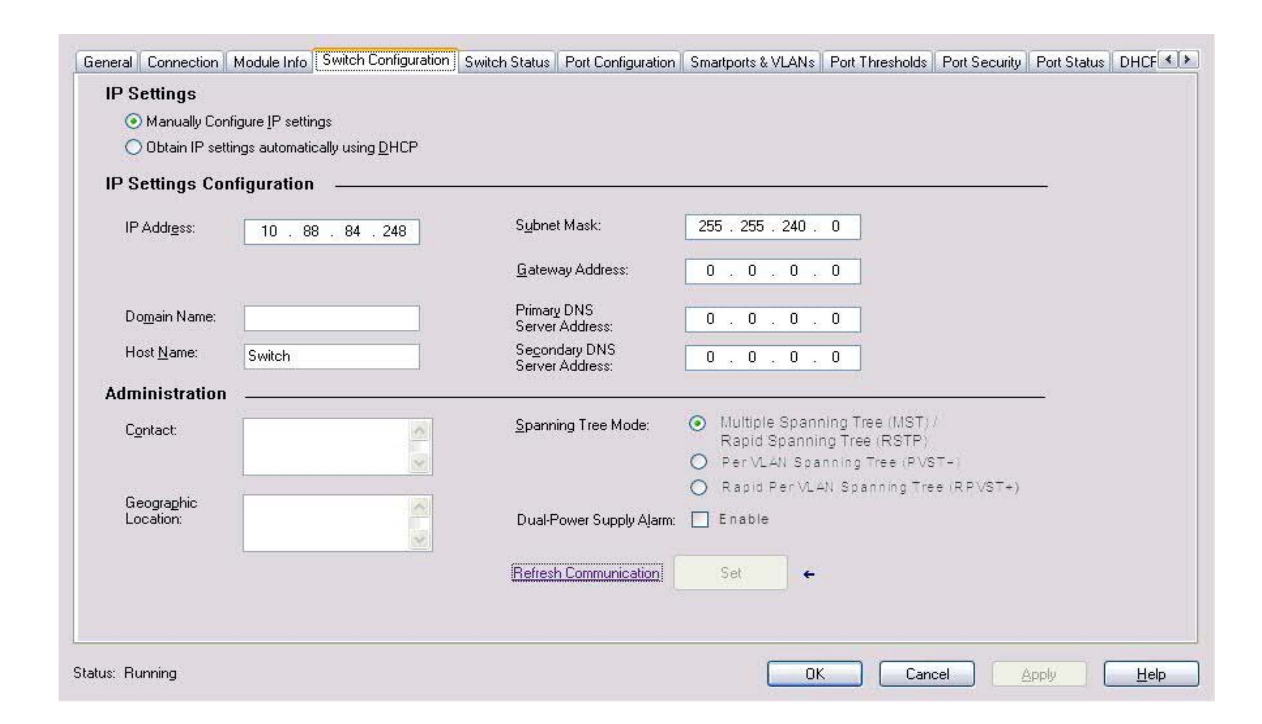


Tabla 29 - Campos de la ficha Switch Configuration

Campo	Descripción
IP Address	Este valor debe coincidir con la dirección IP de la ficha General. Si reconfigura el switch con una dirección IP diferente, es posible que pierda la comunicación con el switch al hacer clic en Set. Para corregir este problema, deberá volver a la ficha General de Express Setup, definir la nueva dirección IP y descargar al controlador.
Subnet Mask	Escriba la máscara de subred adecuada para el switch. La máscara de subred es un número de 32 bits. Defina cada octeto entre 0 y 255. El valor predeterminado es 255.255.255.0.
Gateway Address	Un gateway es un encaminador u otro dispositivo de red a través del cual el switch se comunica con dispositivos de otras redes o subredes. La dirección IP del gateway debe formar parte de la misma subred que la dirección IP del switch. La dirección IP del switch y la dirección IP del gateway predeterminado no pueden ser iguales. **IMPORTANTE:** La comunicación se interrumpe al cambiar la dirección de gateway (IP).
Primary DNS Server Address	Escriba la dirección IP del servidor de nombres de dominio (DNS) primario. Defina cada octeto entre 0 y 255. El primer octeto no puede ser 127 ni un número mayor que 223.
Secondary DNS Server Address	Escriba la dirección IP del servidor de nombres de dominio (DNS) secundario. Defina cada octeto entre 0 y 255. El primer octeto no puede ser 127 ni un número mayor que 223.
Domain Name	Escriba el nombre del dominio en el que reside el módulo. El nombre de dominio consiste en una secuencia de etiquetas de nombres separadas por puntos, como ejemplo.com. El nombre de dominio tiene un límite de 48 caracteres y se restringe a las letras ASCII a…z, los dígitos 0…9, y puntos y guiones.
Host Name	(Opcional). Escriba un nombre que le ayude a identificar el switch para monitorearlo o resolver un problema. El nombre puede tener un máximo de 64 caracteres y puede incluir caracteres alfanuméricos y especiales (coma y raya).
Contact	(Opcional). Escriba la información de contacto del switch, hasta un máximo de 200 caracteres. La información de contacto puede incluir caracteres alfanuméricos y especiales (raya y coma), así como un retorno de carro.
Geographic Location	(Opcional). Escriba la ubicación geográfica del switch, hasta un máximo de 200 caracteres. La ubicación geográfica puede incluir caracteres alfanuméricos y especiales (raya y coma), así como un retorno de carro.
Spanning Tree Mode	Elija uno de los siguientes: • RSTP/MST • PVST+ • RPVST+ RSTP/MST es el valor predeterminado.
Dual-Power Supply Alarm	Marque la casilla de selección para habilitar esta característica. Esta característica está inhabilitada de manera predeterminada.
Refresh	Haga clic para actualizar la ficha con nuevos datos del switch.
Set	Haga clic para guardar los ajustes en el switch y en la tarjeta SD, si se ha insertado. Una vez que se haya especificado correctamente la contraseña, se pueden realizar cambios durante 10 minutos sin que el cuadro de diálogo Enter Password le pida la contraseña.

Estado del switch

En la ficha Switch Status, puede ver varios parámetros de estado relativos al switch.

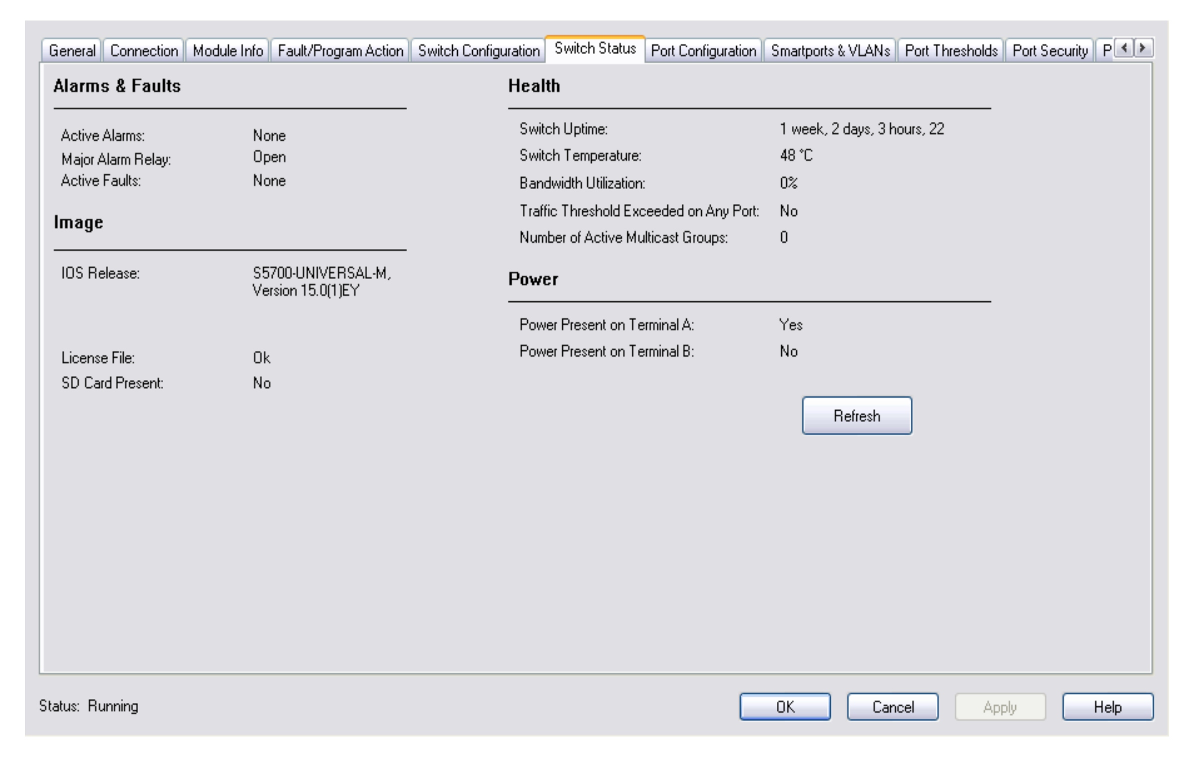


Tabla 30 - Campos de la ficha Switch Status

Campo	Descripción
Active Alarms	Muestra uno de estos valores: • None • Port alarm • Dual Mode Power Supply alarm • Primary Temperature alarm
Major Alarm Relay	Muestra uno de estos valores: • Open • Closed
Active Faults	Muestra uno de estos valores: • None • Port fault • Hardware fault Si los fallos de puerto y hardware están activos, aparecerá el estado de fallo de hardware.
Traffic Threshold Exceeded on Any Port	Muestra un valor Yes o No que indica si se han excedido los umbrales actuales de unidifusión, multidifusión y difusión en cualquier puerto. Para ver el estado de los puertos activos, haga clic en la ficha Port Status. Para ver los valores de umbral, haga clic en la ficha Advanced - Port Threshold.
Switch Uptime	Muestra los días, horas y minutos que el switch ha funcionado desde el último reinicio.
Switch Temperature	Muestra la temperatura interna actual (en grados centígrados) del switch.
Bandwidth Utilization	Muestra el porcentaje total de ancho de banda del switch que se está utilizando.
Power Present on Terminal A	Muestra un valor Yes o No que indica si hay alimentación en el terminal A.
Power Present on Terminal B	Muestra un valor Yes o No que indica si hay alimentación en el terminal B.
Number of Active Multicast Groups	Muestra el número de grupos de multidifusión activos.
IOS Release	Muestra la versión actual del sistema operativo del switch.

Port Configuration

Los ajustes de configuración de los puertos determinan la forma en que se reciben y se envían los datos entre el switch y el dispositivo conectado.

Debe estar en línea para configurar las características de los puertos. La mayor parte de la información de esta ficha no aparece si está fuera de línea.

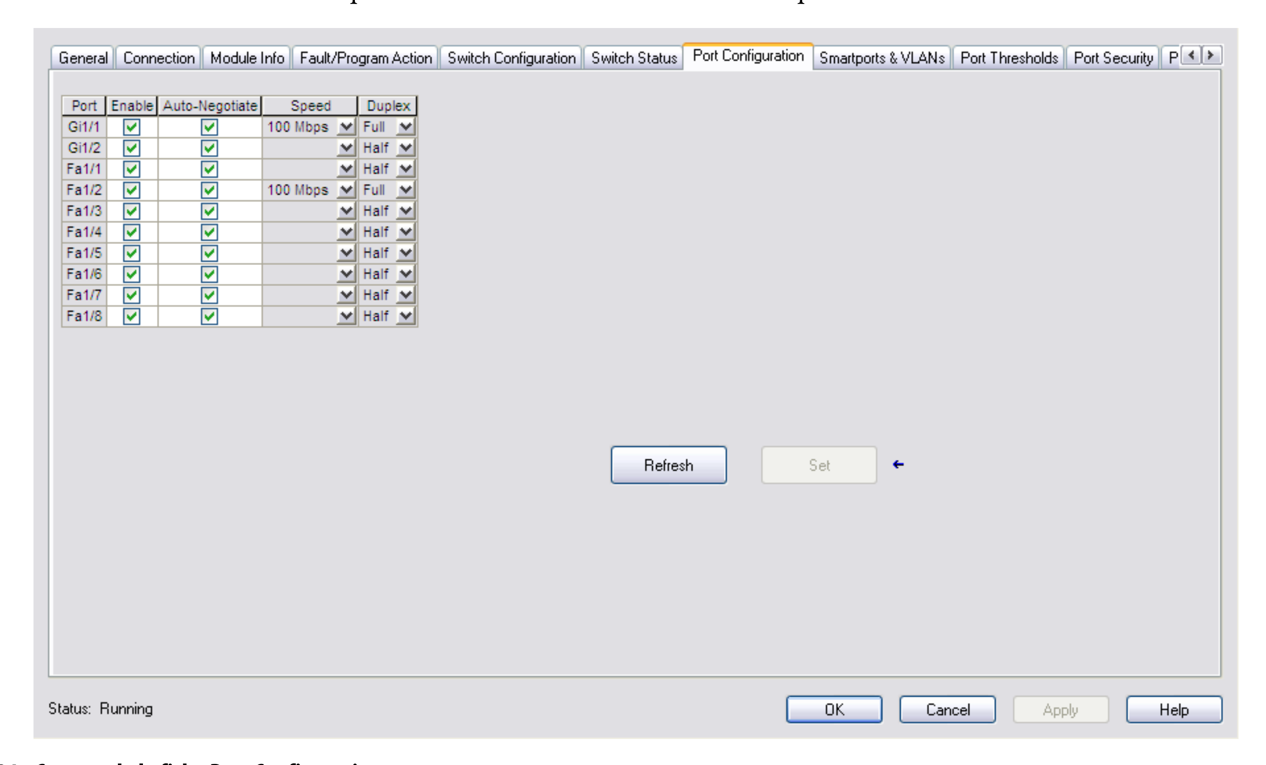


Tabla 31 - Campos de la ficha Port Configuration

Campo	Descripción
Port	Puerto seleccionado para la configuración. El número de puerto incluye el tipo de puerto (Fa para Fast Ethernet y Gi para Gigabit Ethernet) y el número de puerto específico. **EJEMPLO:** Gi1/1 es el puerto Gigabit Ethernet 1.
Enable	Marque la casilla de selección para habilitar el puerto. Desmarque la casilla de selección para inhabilitar (apagar) manualmente el puerto. Le recomendamos que inhabilite el puerto si no lo está utilizando y no está conectado a ningún dispositivo. Puede inhabilitar manualmente el puerto para trabajar en un problema relacionado con una conexión bajo sospecha de no estar autorizada.
Auto-negotiate	Marque la casilla de selección si desea que el puerto y el dispositivo final autonegocien la velocidad del vínculo y el modo dúplex. Desmarque la casilla de selección para especificar manualmente la velocidad del puerto y el modo dúplex que desee. Le recomendamos que utilice el valor predeterminado (autonegociar) para que los ajustes de velocidad y dúplex del puerto del switch coincidan automáticamente con los ajustes del dispositivo conectado. Cambie la velocidad y el modo dúplex del puerto del switch si el dispositivo conectado requiere una velocidad y un modo dúplex específicos. Si define la velocidad y el modo dúplex para el puerto del switch, también se deberá configurar el dispositivo conectado con exactamente los mismos valores de velocidad y modo dúplex, y no deberá establecerse en autonegociar, ya que de otra manera se producirá una desigualdad de velocidad/modo dúplex. Las interfaces de fibra óptica no admiten la autonegociación.
Speed	Elija la velocidad de funcionamiento del puerto. Gigabit (Gi): • 10 Mbps • 100 Mbps • 1 Gbps Fast Ethernet (Fa): • 10 Mbps • 100 Mbps
Duplex	Elija uno de estos modos dúplex: • Half-duplex: ambos dispositivos no pueden enviar datos al mismo tiempo. Half-duplex no está disponible cuando la velocidad se establece en 1 Gbps. • Full-duplex: ambos dispositivos pueden enviar datos al mismo tiempo.

Smartports y redes VLAN

En la ficha Smartports & VLANs, puede asignar roles Smartport y redes VLAN a los puertos del switch. También puede crear, editar y eliminar redes VLAN. Debe estar en línea para configurar estas características de los puertos. La mayor parte de la información de esta ficha no aparece si está fuera de línea.

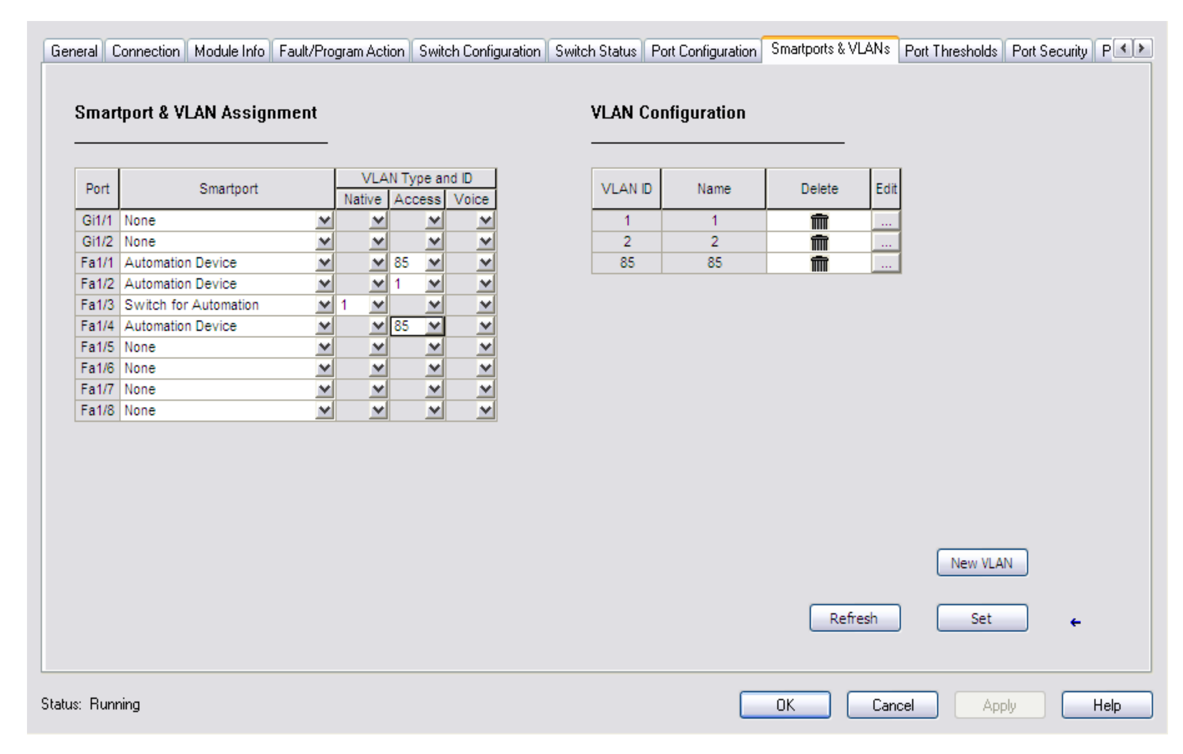


Tabla 32 - Campos de la ficha Smartports and VLANs

Campo	Descripción
Port	Puerto seleccionado para la configuración. El número de puerto incluye el tipo de puerto (Fa para Fast Ethernet y Gi para Gigabit Ethernet) y el número de puerto específico. **EJEMPLO:** Gi1/1 es el puerto Gigabit Ethernet 1.
Smartport	Los roles Smartport son las configuraciones recomendadas para los puertos. Estas configuraciones se denominan roles de puertos. Optimizan las conexiones del switch y proporcionan seguridad, transmisiones de calidad y fiabilidad en el tráfico de los puertos del switch. Estas configuraciones también previenen muchos problemas ocasionados por errores de configuración de los puertos. Los roles de puertos dependen del tipo de dispositivo que se conecta al puerto del switch. Debe decidir el tipo de dispositivo que se conectará a cada puerto antes de elegir un rol Smartport. Elija uno de estos roles Smartport para aplicarlo al puerto conectado: • Automation Device: aplique este rol a los puertos que se van a conectar a dispositivos EtherNet/IP. Se puede usar para dispositivos de automatización industrial, como controladores lógicos y E/S. – El puerto está establecido en el modo Access. – La seguridad del puerto solo admite una ID MAC. – Optimiza la administración de colas para el tráfico CIP. • Desktop for Automation: aplique este rol a los puertos que se van a conectar a dispositivos de escritorio como, por ejemplo, computadoras de escritorio, estaciones de trabajo, computadoras portátiles y otros anfitriones basados en clientes: No aplique este rol a puertos que se van a conectar a switches, encaminadores o puntos de acceso. – El puerto está establecido en el modo Access. – Portfast habilitado. – La seguridad del puerto solo admite una ID MAC. • Switch for Automation: aplique este rol a los puertos que se van a conectar a otros switches. – El puerto está establecido en el modo Trunk. – Portfast habilitado. • Router for Automation: aplique este rol a los encaminadores o puertos que se van a conectar a switches de capa 3 con servicios de encaminamiento habilitados. • Phone for Automation: aplique este rol a los puertos que se van a conectar a teléfonos IP. Se puede conectar al teléfono IP un dispositivo de escritorio como, por ejemplo, una computadora. Tanto el teléfono IP como la computadora conectada pueden obtener acceso a la red a través del puerto. Este rol da prioridad al tráfico de voz sobre el tráfico general de datos para proporcionar una recepción clara de la voz en los teléfonos IP. – El puerto está establecido en el modo Trunk. – La seguridad del puerto admite tres ID MAC para este puerto. • Wireless For Automation: aplique este rol a los puertos que se van a conectar a puntos de acceso inalámbricos. El punto de acceso proporciona acceso a la red a un máximo de 30 usuarios móviles (inalámbricos). • Port Mirroring: aplique este rol a los puertos que se van a monitorear mediante un analizador de red. Para obtener más información acerca de puertos espejo, consulte Puerto espejo en la página 91. • None: aplique este rol a los puertos si no desea tener un rol Smartport especializado en el puerto. Este rol se puede usar en las conexiones con cualquier dispositivo, incluidos dispositivos en los roles antes descritos. • Custom: cree estos roles para su aplicación. Puede definir el tipo de VLAN que implemente, si corresponde. – Escriba el nombre de la macro. En los nombres de las macros se distingue entre mayúsculas y minúsculas. La cadena puede tener hasta 31 caracteres alfanuméricos, que no pueden incluir un signo ?, un espacio ni un tabulador. – Elija el icono de la macro (de CS1 a CS10).
VLAN Configuration	Muestra la ID y el nombre de VLAN: • VLAN ID: identificador único (en el rango de 2…4094; los valores de 1002 a 1005 están reservados) de una VLAN que haya creado mediante un clic en Add New VLAN. VLAN ID 1 es el valor predeterminado. • Name: nombre único de la VLAN (20 caracteres como máximo) que haya creado mediante un clic en Add New VLAN.

Umbrales de puerto

En la ficha Port Thresholds, puede configurar los límites de umbral para el tráfico de difusión, unidifusión y multidifusión en cada puerto activo. Esta característica solo está disponible con el firmware completo. Se compara el número de paquetes enviados con el valor del umbral. Estos límites ayudan a evitar que un solo dispositivo envíe demasiado tráfico. Para obtener más información acerca de esta característica, consulte Umbrales de puertos en la página 74.

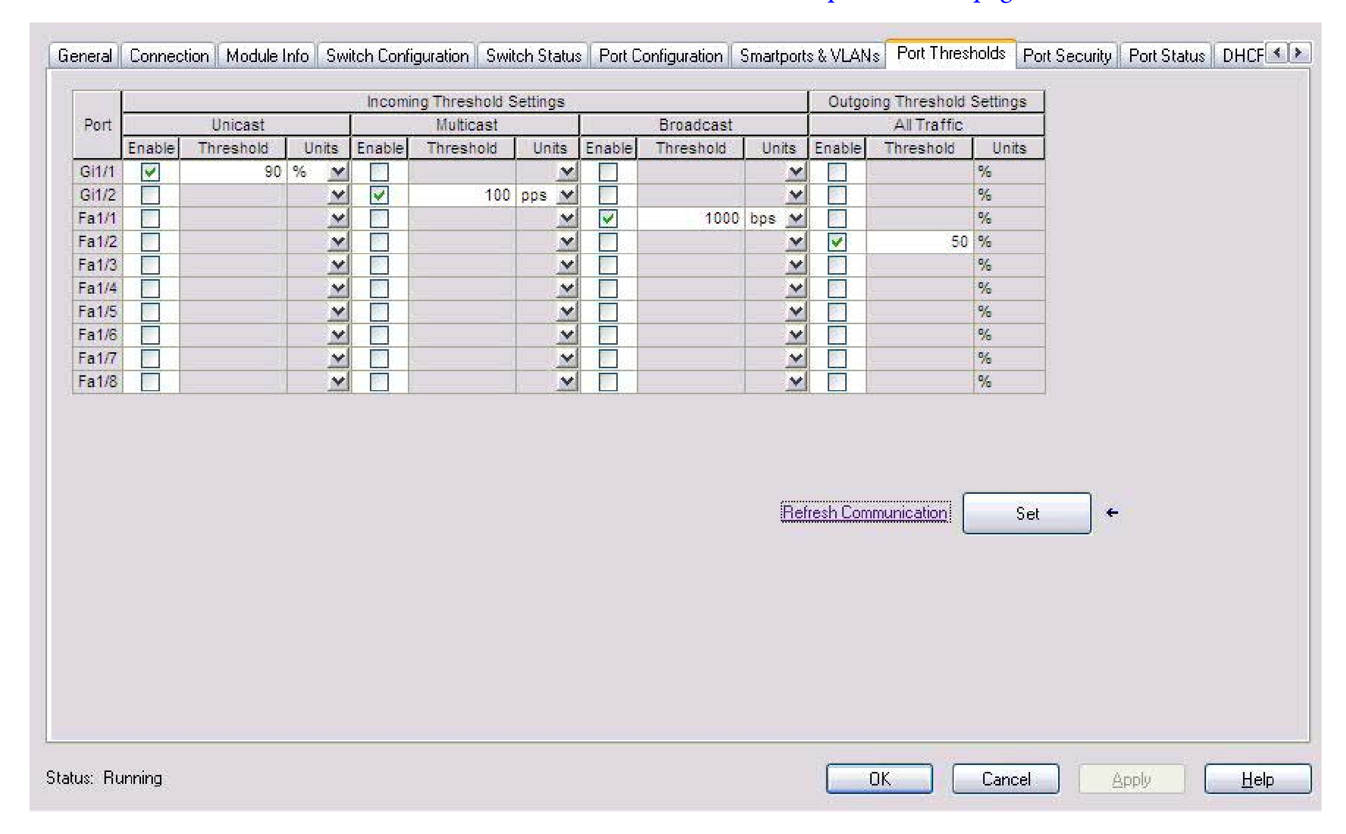


Tabla 33 - Campos de la ficha Port Threshold

Campo	Descripción
Port	Puerto seleccionado para la configuración. El número de puerto incluye el tipo de puerto (Fa para Fast Ethernet y Gi para Gigabit Ethernet) y el número de puerto específico. **EJEMPLO:** Gi1/1 es el puerto Gigabit Ethernet 1.
Incoming Threshold Settings	Habilite los umbrales entrantes y defina los valores de umbral para el tráfico de unidifusión, multidifusión y difusión para cada puerto. Valores válidos para las unidades: • Paquetes por segundo (pps) • Porcentaje del ancho de banda total (%) • Bits por segundo (bps)
Outgoing Threshold Settings	Habilite los umbrales salientes y defina los valores de umbral para el tráfico para cada puerto. Units % = Porcentaje del ancho de banda total

Seguridad de puertos

La característica de seguridad de puertos solo se aplica al firmware completo. Para obtener más información, consulte Seguridad de puertos en la página 76.

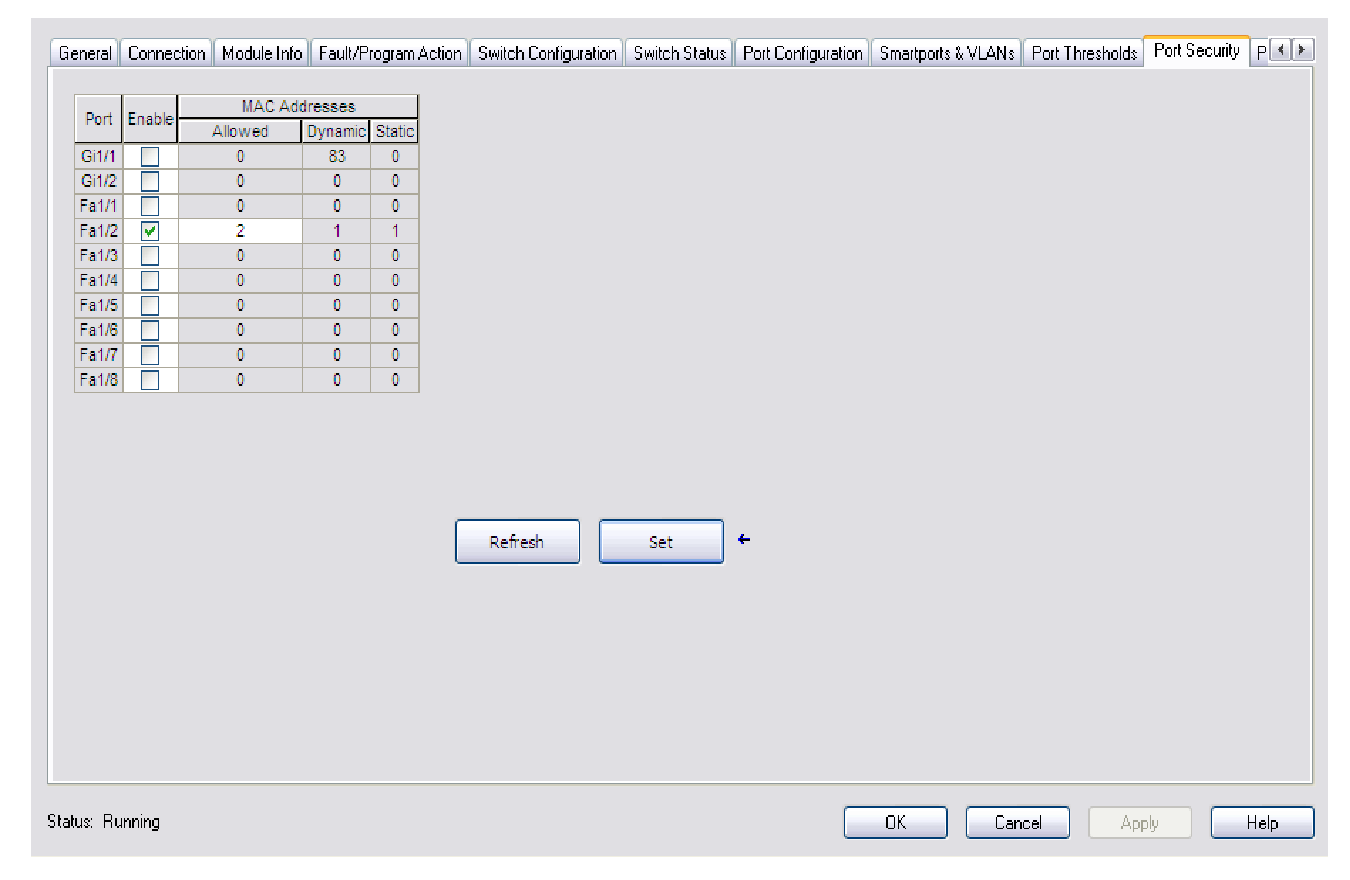


Tabla 34 - Campos de la ficha Port Security

Campo	Descripción
Port	Puerto en el que desea habilitar o inhabilitar la seguridad.
Enable	Marque la casilla de selección para habilitar la seguridad del puerto.
MAC Addresses	Número de direcciones MAC dinámicas o estáticas admitidas. • Permitidas: 1…80. • Dynamic: número de direcciones MAC (dispositivos) conectadas actualmente al puerto que no se definen manualmente (estáticamente). • Static: número de direcciones MAC (dispositivos) definidas estáticamente mediante la interface web del administrador de dispositivos. Observe que este número debe ser mayor que la suma de estáticas + dinámicas para un determinado puerto. Si desea definir el número en un valor inferior, desconecte los dispositivos adecuados y deje que sus entradas en la tabla de seguridad de puertos sobrepasen el tiempo de espera.

Port Status

La ficha Port Status le permite monitorear alarmas, estados, umbrales y utilización del ancho de banda. También puede ver los diagnósticos de puertos y de cables.

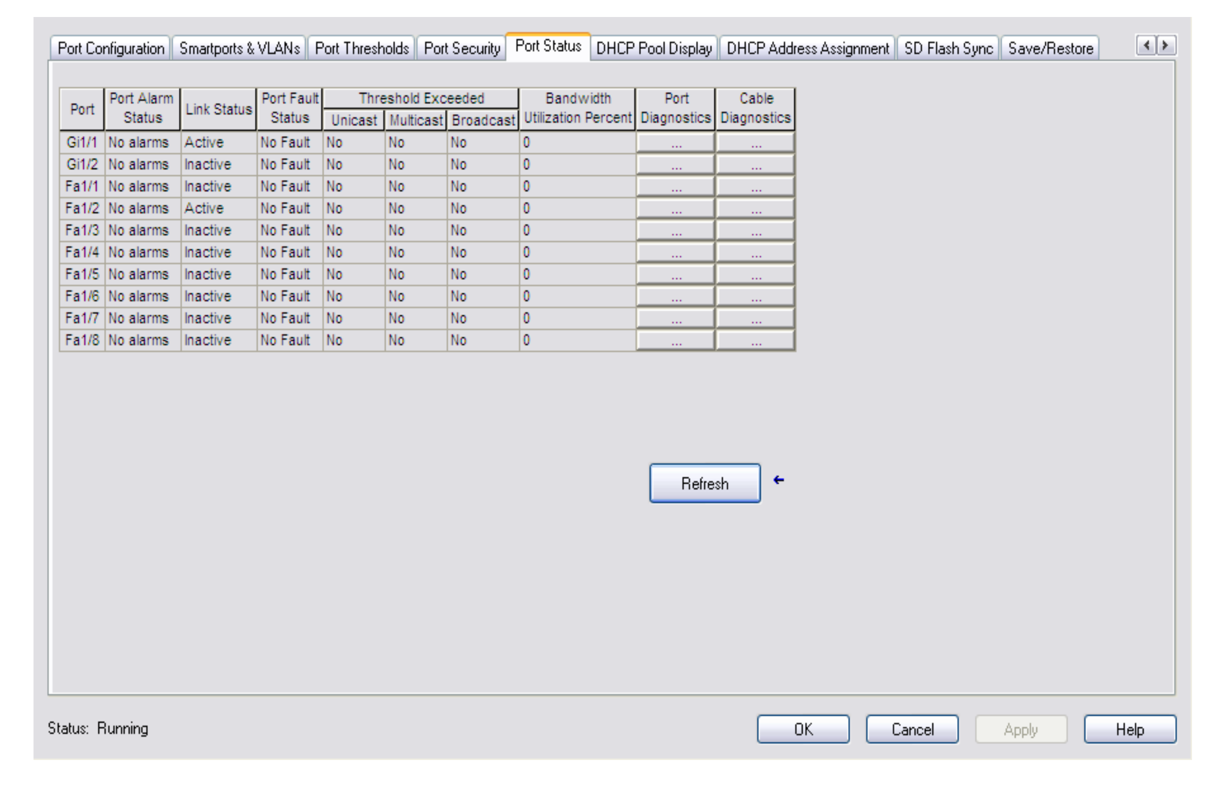


Tabla 35 - Campos de la ficha Port Status

Campo	Descripción
Port	Muestra el puerto seleccionado. El número de puerto incluye el tipo de puerto (Fa para Fast Ethernet y Gi para Gigabit Ethernet) y el número de puerto específico. **EJEMPLO:** Gi1/1 es el puerto Gigabit Ethernet 1.
Port Alarm Status	Muestra el estado actual de la alarma del puerto. Valores válidos: • Link fault alarm • Port not forwarding alarm • Port not operating alarm • High bit error rate alarm • No alarms
Link Status	Muestra si el vínculo está activo o inactivo.
Port Fault Status	Muestra el estado actual de la alarma del puerto. Valores válidos: • Error - Disable event • SFP error - Disabled • CDP native VLAN mismatch • MAC address flap • Port security violation • No fault
Threshold Exceeded	Muestra cambios inusuales para los siguientes tipos de tráfico de red: • Unicast: muestra un valor Yes o No que indica si el tráfico de unidifusión actual ha excedido el valor del umbral. • Multicast: muestra un valor Yes o No que indica si el tráfico de multidifusión actual ha excedido el valor del umbral. • Broadcast: muestra un valor Yes o No que indica si el tráfico de difusión actual ha excedido el valor del umbral.
Bandwidth Utilization Percent	Muestra el porcentaje de ancho de banda que se está utilizando. Observe si el porcentaje del uso es el esperado durante el período de actividad determinado de la red. Si el uso es superior al esperado, es posible que haya un problema.
Port Diagnostics	Haga clic para abrir el cuadro de diálogo Port Diagnostics para el puerto correspondiente. El cuadro de diálogo Port Diagnostics le proporciona información para diagnosticar un problema de rendimiento de la red.
Cable Diagnostics	Haga clic para abrir el cuadro de diálogo Cable Diagnostics para el puerto correspondiente. El cuadro de diálogo Cable Diagnostics le proporciona información para diagnosticar un problema de cable.

Port Diagnostics

Utilice el cuadro de diálogo Port Diagnostics para ver el estado del rendimiento del vínculo:

- Ver contadores de octetos y paquetes
- Ver colisiones en el vínculo
- Ver errores en el vínculo
- Restablecer y borrar todos los contadores de estado

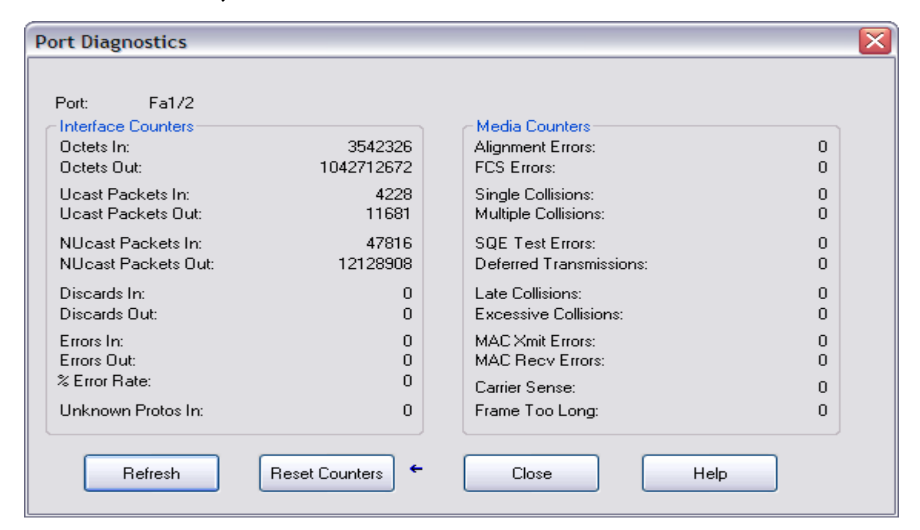
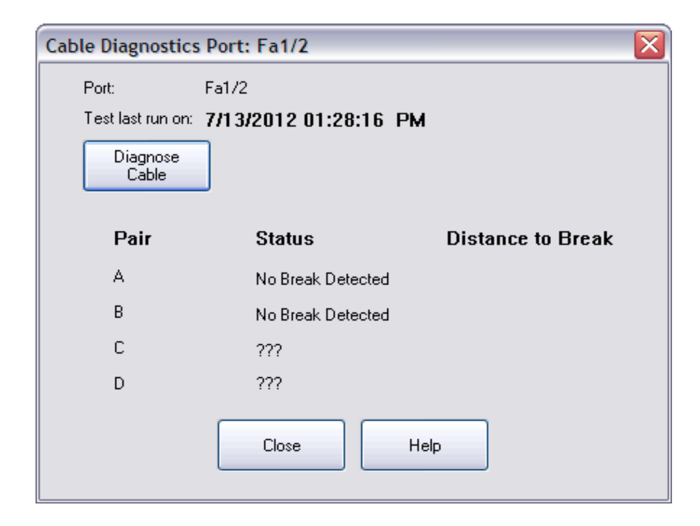


Tabla 36 - Campos del cuadro de diálogo Port Diagnostics

Campo	Descripción
Port	Puerto seleccionado para la configuración. El número de puerto incluye el tipo de puerto (Fa para Fast Ethernet y Gi para Gigabit Ethernet) y el número de puerto específico. **EJEMPLO:** Gi1/1 es el puerto Gigabit Ethernet 1.
Interface Counters	Estos contadores le permiten ver el estado de los octetos recibidos y enviados, así como de los paquetes recibidos y enviados: • Octets In: número de octetos recibidos por el puerto. • Octets Out: número de octetos enviados por el puerto. • Ucast Packets In: número de paquetes de unidifusión recibidos por el puerto. • Ucast Packets Out: número de paquetes de unidifusión enviados por el puerto. • NUcast packets In: número de paquetes de multidifusión recibidos por el puerto. • NUcast packets Out: número de paquetes de multidifusión enviados por el puerto. • Discards In: número de paquetes entrantes que han sido descartados. • Discards Out: número de paquetes salientes que han sido descartados. • Errors In: número de paquetes entrantes que contienen errores. • Errors Out: número de paquetes salientes que contienen errores. • Unknown Protos (Protocols) In: número de paquetes entrantes con protocolos desconocidos.
Media Counters	Estos contadores le permiten ver el número de colisiones de un vínculo: • Single: número de colisiones sencillas. • Multiple: número de colisiones múltiples. • Late: número de colisiones tardías. • Excessive: número de tramas cuya transmisión falla a consecuencia de un número excesivo de colisiones. • Estos contadores le permiten ver los errores: • Alignment: número de tramas recibidas cuya longitud no es un número entero de octetos. • FCS (Frame Check Sequence): número de tramas recibidas con fallo en la comprobación FCS. • SQE Test Errors: número de veces que se ha generado el mensaje SQE TEST ERROR. • Deferred Transmissions: conteo de transmisiones postergadas debido a que la red está ocupada. • MAC Xmit Errors: número de tramas que no se han podido transmitir a consecuencia de un error de transmisión de subcapa MAC interna. • MAC Recv Errors: número de tramas que no se han podido recibir a consecuencia de un error de recepción de subcapa MAC interna. • Carrier Sense: número de veces que la condición de detección de portadora se perdió o no se produjo nunca al intentar transmitir una trama. • Frame Too Long: número de tramas recibidas que exceden el tamaño máximo de trama permitido.

Diagnóstico de cables

El cuadro de diálogo Cable Diagnostics le proporciona información para diagnosticar un problema de cable.



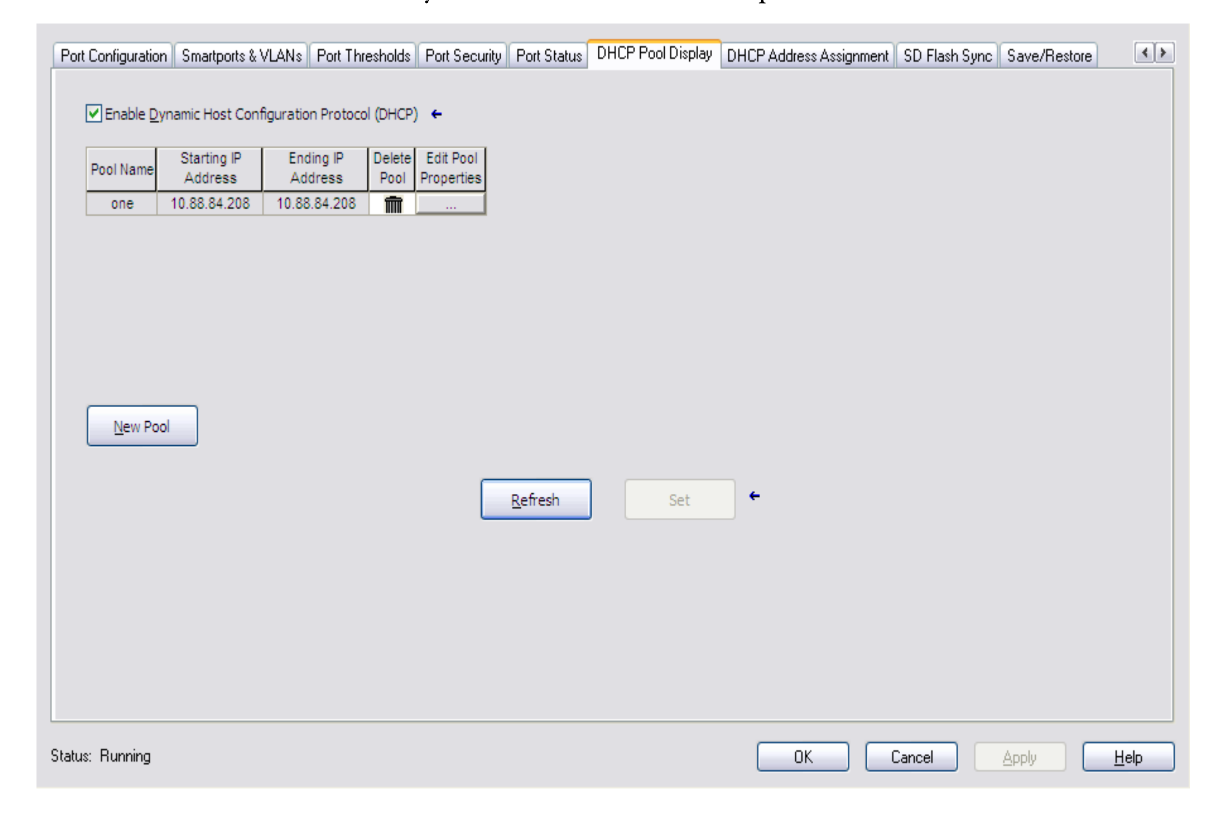
SUGERENCIA La información de esta ficha no aparece si está fuera de línea.

Tabla 37 - Campos del cuadro de diálogo Cable Diagnostics Port

Campo	Descripción
Port	Puerto seleccionado para la configuración. El número de puerto incluye el tipo de puerto (Fa para Fast Ethernet y Gi para Gigabit Ethernet) y el número de puerto específico. **EJEMPLO:** Gi1/1 es el puerto Gigabit Ethernet 1.
Test last run on	Hora a la que se ejecutó por última vez la prueba. El formato de fecha y hora es mm/dd/aa hh:mm:ss tt. Si no se ha ejecutado nunca la prueba, la hora y toda la información sobre distancia y estado aparecerán en blanco.
Pair	Cada par (par de cables de la red) listado por separado. Si no existe el par o la prueba no se ha ejecutado nunca, aparece en blanco.
Status	Especifica el estado del vínculo la última vez que se ejecutó la prueba. Si no existe el par o la prueba no se ha ejecutado, el estado aparece en blanco. Para la distancia, si el par está en estado normal, se muestra 'No Break Detected'. No se muestra ninguna distancia.
Distance to Break	La distancia desde el switch hasta la interrupción para cada par estimado, con un valor de error aproximado, listado de manera individual. Solo aparece un valor si el estado de un par existente no es Normal. Este campo aparece en blanco si no se ha ejecutado nunca antes una prueba. Si no existe un par, se muestra '???'.
Diagnose Cable	Haga clic para ejecutar la prueba de diagnóstico de cable. Aparecerá una advertencia de interrupción de la conexión: • Si está seguro de que desea continuar con la prueba, haga clic en Yes. Debe estar preparado para escribir una contraseña válida a fin de ejecutar la prueba. • Si no desea ejecutar la prueba, haga clic en No o cierre la ventana. **IMPORTANTE:** Para ejecutar una prueba válida en puertos gigabit, primero debe configurar el puerto gigabit como un tipo de medio físico RJ45 en la interface web del administrador de dispositivos, tal como se describe en Configure los ajustes de puerto en la página 109. **IMPORTANTE:** Esta prueba puede interrumpir conexiones a este módulo y a cualquier otro módulo conectado a través de este módulo. Además, se puede interrumpir la conexión entre la estación de trabajo y el controlador. Debe disponer del privilegio adecuado para ejecutar esta prueba.

Visualice grupos de DHCP

Puede ver información de los grupos de direcciones de DHCP del switch mediante la ficha DHCP Pool Display. Puede ver de 0 a 15 grupos. Esta información se extrae directamente del switch. Cada fila representa una única ocurrencia y los valores de ocurrencias no pueden ser consecutivos.



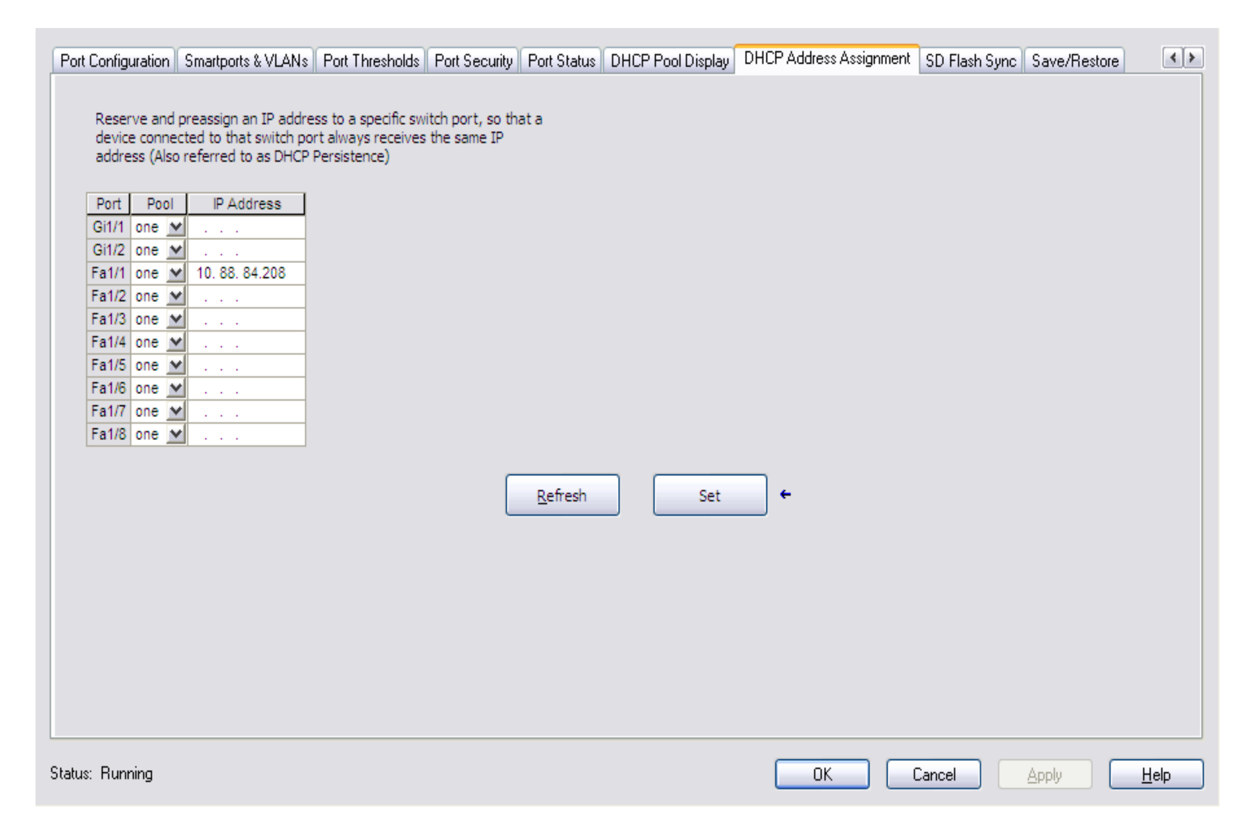
SUGERENCIA La información de esta ficha no aparece si está fuera de línea.

Tabla 38 - Campos de la ficha DHCP Pool Display

Campo	Descripción
Enable Dynamic Host Configuration Protocol (DHCP)	Habilita o inhabilita los grupos. Si está marcada, todos los controles de la cuadrícula se definen en línea y los valores adecuados se obtienen del switch y se muestran. Si está desmarcada, todos los controles de la cuadrícula se definen fuera de línea. Presione Alt - D en el teclado.
Pool Name	Muestra el nombre del grupo de direcciones IP de DHCP configurado en el switch. Un grupo de direcciones IP de DHCP es un rango (o grupo) de direcciones IP disponibles que el switch puede asignar a los dispositivos conectados. El nombre puede tener un máximo de 31 caracteres alfanuméricos, que no pueden incluir un signo ? ni un tabulador.
Starting IP Address	Muestra la dirección IP inicial que define el rango de direcciones del grupo de direcciones IP de DHCP. El formato consiste en una dirección numérica de 32 -bits escrita como cuatro números separados por puntos (por ejemplo, 255.255.255.255). Cada número puede estar entre 0 y 255.
Ending IP Address	Muestra la dirección IP final que define el rango de direcciones del grupo de direcciones IP de DHCP. El formato consiste en una dirección numérica de 32 bits escrita como cuatro números separados por puntos (por ejemplo, 255.255.255.255). Cada número puede estar entre 0 y 255.
Delete Pool	Haga clic para eliminar la fila del grupo de DHCP seleccionada actualmente. A continuación, si hace clic en Set, aparecerá un cuadro de diálogo de confirmación y también se eliminarán todas las direcciones persistentes asociadas con la fila del grupo de DHCP seleccionada. Delete Pool solo está disponible cuando el switch está en línea, se ha marcado la casilla de selección Enable Dynamic Host Configuration Protocol (DHCP) y la fila correspondiente contiene datos. Delete Pool aparecerá atenuado si el switch está fuera de línea y la casilla de selección Enable Dynamic Host Configuration Protocol (DHCP) no está marcada.
Refresh	Haga clic para actualizar el control de cuadrícula con nuevos datos obtenidos directamente del switch. Presione Alt-R en el teclado. Si ha cambiado un valor de la cuadrícula y hace clic en Refresh antes de hacer clic en Set, todos los valores de la cuadrícula regresarán a sus valores anteriormente definidos. Refresh solo está disponible cuando el switch está en línea. El botón Refresh aparece atenuado cuando el switch está fuera de línea.
Edit Pool Properties	Haga clic para abrir el cuadro de diálogo DHCP Pool Definition and Edit y rellenarlo con los valores de la ocurrencia correspondiente a la fila actual. El botón de la columna Edit solo está disponible cuando el switch está en línea, se ha marcado la casilla de selección Enable Dynamic Host Configuration Protocol (DHCP) y la fila correspondiente contiene datos. El botón de la columna Edit aparecerá atenuado si el switch está fuera de línea y la casilla de selección Enable Dynamic Host Configuration Protocol (DHCP) no está marcada.
New Pool	Haga clic para abrir el cuadro de diálogo DHCP Pool Definition and Edit (todos los campos están en blanco y el botón de radio Custom no está seleccionado). Además, se añadirá una nueva fila/ocurrencia a la cuadrícula en el cuadro de diálogo Module Properties - DHCP Pool Display. Presione Alt - N en el teclado. El botón New solo está disponible cuando el switch está en línea y se ha seleccionado la casilla de selección Enable Dynamic Host Configuration Protocol (DHCP). El botón New aparecerá atenuado si el switch está fuera de línea y la casilla de selección Enable Dynamic Host Configuration Protocol (DHCP) no está marcada.
Set	Haga clic para aplicar al switch los cambios realizados a los atributos de este cuadro de diálogo. Solo se aplicarán al switch aquellos atributos que se hayan modificado. Es posible que aparezca el cuadro de diálogo Enter Password. Si se produce un error al definir un atributo, finalizará la operación Set y no se aplicará al switch el resto de los valores de los atributos. Además, el botón Set seguirá estando disponible. El botón Set solo está disponible cuando el switch está en línea y se ha cambiado el valor de cualquiera de los atributos. El botón Set aparece atenuado cuando el switch está fuera de línea.

Asignación de direcciones de DHCP

Puede ver y configurar la persistencia de DHCP desde la ficha DHCP Address Assignment. Con la persistencia de DHCP, se puede asignar una dirección IP específica a cada puerto para que el dispositivo conectado a un puerto específico reciba la misma dirección IP.



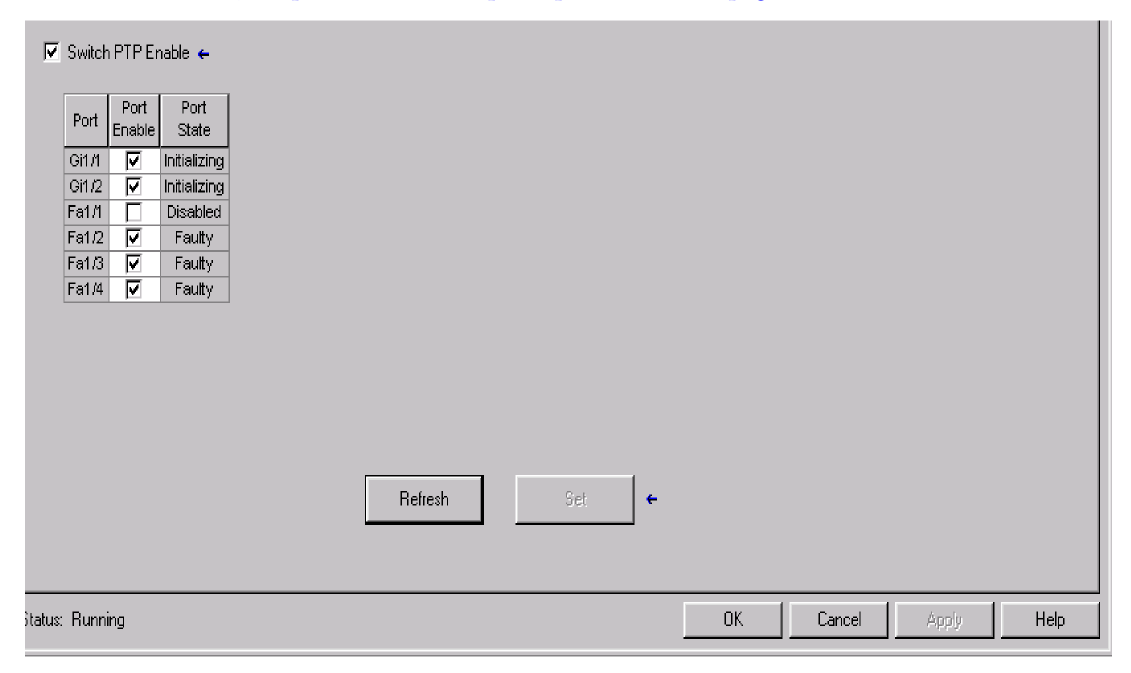
SUGERENCIA La información de esta ficha no aparece si está fuera de línea.

Tabla 39 - Campos de la ficha DHCP Address Assignment

Campo	Descripción
Port	Muestra los puertos disponibles para la configuración. El número de puerto incluye el tipo de puerto (Fa para Fast Ethernet y Gi para Gigabit Ethernet), el número de switch (1) y el número de puerto específico. **EJEMPLO:** • Gi1/1 es el puerto Gigabit Ethernet 1. • Fa1/1 es el puerto Fast Ethernet 1.
Pool	Muestra los nombres de los grupos de direcciones IP de DHCP que corresponden a las ocurrencias disponibles en el switch. Si elimina todas las filas que contienen grupos en la ficha DHCP Pool Display del cuadro de diálogo Module Properties y hace clic en Refresh, el campo Pool aparecerá en blanco. El campo Pool está disponible cuando el switch está en línea y aparece atenuado cuando el switch está fuera de línea.
IP Address	Muestra la dirección IP asignada al puerto del switch. El formato consiste en una dirección numérica de 32 bits escrita como cuatro números separados por puntos (por ejemplo, 255.255.255.255). Cada número puede estar entre 0 y 255. El campo IP Address solo está disponible cuando el switch está en línea y aparece atenuado cuando el switch está fuera de línea.
Refresh	Haga clic para actualizar el control de cuadrícula con nuevos datos obtenidos directamente del switch. Presione Alt-R en el teclado. Si ha cambiado un valor de la cuadrícula y hace clic en Refresh antes de hacer clic en Set, todos los valores de la cuadrícula regresarán a sus valores anteriormente definidos. El botón Refresh solo está disponible cuando el switch está en línea. El botón Refresh aparece atenuado cuando el switch está fuera de línea.
Set	Haga clic para aplicar al switch los cambios realizados en este cuadro de diálogo. Es posible que aparezca el cuadro de diálogo Enter Password.

Time Sync Configuration

Utilice esta característica para sincronizar los puertos mediante el PTP. El PTP sincroniza con exactitud de nanosegundos los relojes en tiempo real de los dispositivos de una red. Al utilizar la selección del mejor reloj maestro, el switch identifica el puerto del switch que está conectado a un dispositivo con la mejor fuente de reloj. A continuación, el switch sincroniza su reloj interno con la mejor fuente de reloj y el puerto del switch para definir el estado Master. La fuente de reloj más precisa de la red se denomina reloj Grandmaster. Para obtener más información acerca de esta característica, consulte Sincronización de hora CIP Sync (protocolo de tiempo de precisión) en la página 79.



SUGERENCIA La información de esta ficha no aparece si está fuera de línea.

Tabla 40 - Campos de la ficha Time Sync Configuration

Campo	Descripción
Switch PTP Enable	Marque esta casilla de selección para habilitar el PTP en el dispositivo. De manera predeterminada, el PTP está habilitado en todos los puertos Fast Ethernet y Gigabit Ethernet del switch. Desmarque la casilla de selección para inhabilitar el PTP en el dispositivo. Las características Port Enable y Port State aparecerán atenuadas si la casilla de selección Switch PTP Enable no está marcada.
Port	Muestra el puerto seleccionado para la configuración. El número de puerto incluye el tipo de puerto (Fa para Fast Ethernet y Gi para Gigabit Ethernet) y el número de puerto específico. **EJEMPLO:** Gi1/1 es el puerto Gigabit Ethernet 1.
Port Enable	Marque esta casilla de selección para habilitar la configuración del puerto en el dispositivo. Desmarque la casilla de selección para inhabilitar la configuración del puerto en el dispositivo. La característica Port Enable aparece atenuada si la casilla Switch PTP Enable no está marcada.
Port State	Muestra el estado actual del puerto PTP del dispositivo. Valores válidos: • Initializing • Faulty • Disabled • Listening • Pre-Master • Master • Uncalibrated • Slave El campo Port State aparece en blanco y atenuado si la casilla de selección Switch PTP Enable no está marcada.
Refresh	Haga clic para actualizar la ficha con nuevos datos del switch.
Set	Haga clic para enviar los ajustes al switch. Es posible que aparezca el cuadro de diálogo Enter Password. Debe estar preparado para escribir una contraseña válida a fin de definir los ajustes de configuración. El botón Set aparece atenuado cuando el switch está fuera de línea.

Configuración de NAT

Puede crear ocurrencias de NAT en la ficha NAT.

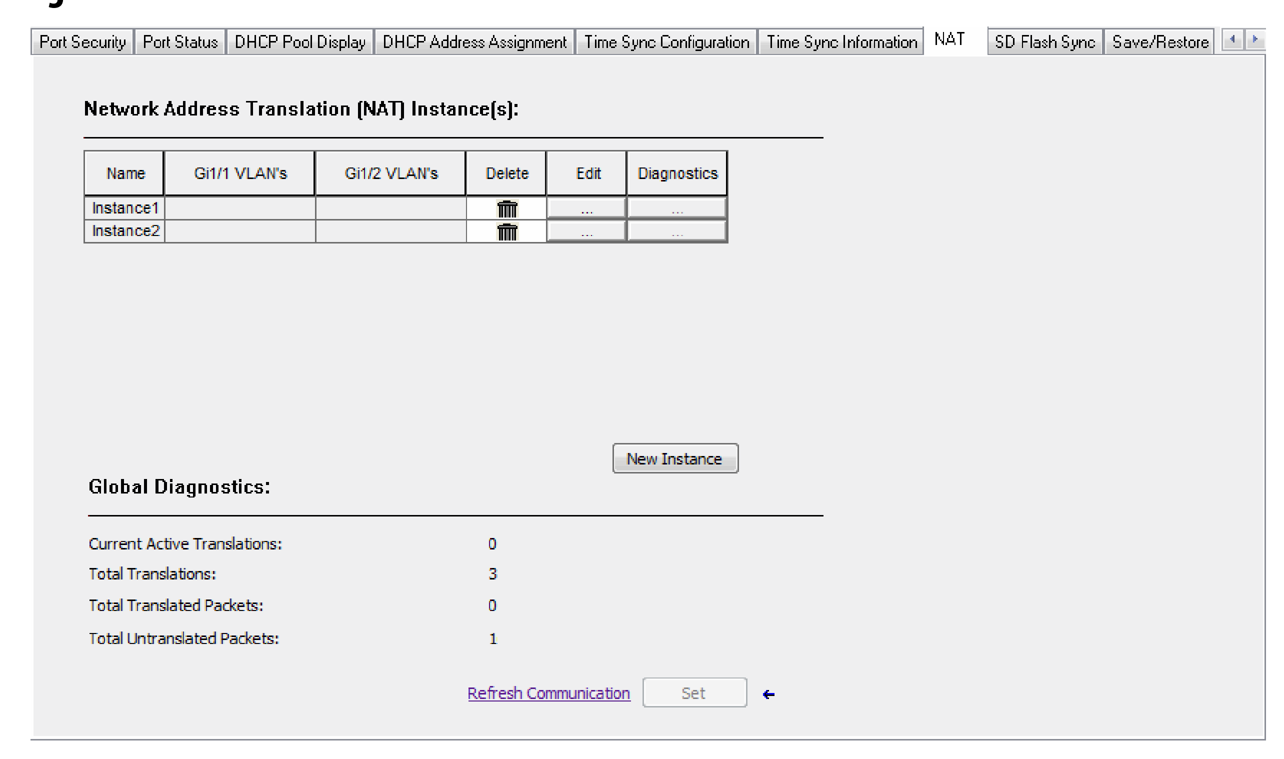


Tabla 41 - Campos de la ficha NAT

Campo	Descripción
Name	Muestra el nombre único de la ocurrencia de NAT.
Gi1/1 VLANs	Muestra las redes VLAN asignadas a cada ocurrencia de NAT en el puerto Gi1/1.
Gi1/2 VLANs	Muestra las redes VLAN asignadas a cada ocurrencia de NAT en el puerto Gi1/2.
Delete	Haga clic para eliminar de manera permanente una ocurrencia de NAT. El switch eliminará la ocurrencia al hacer clic en Set.
Edit	Haga clic para modificar la configuración de una ocurrencia de NAT.
Diagnostics	Haga clic para ver los diagnósticos de traducción de una ocurrencia. Consulte la página 200.
New Instance	Haga clic para crear una ocurrencia de NAT. Consulte la página 188.
Current Active Translations	Muestra el número total de traducciones que se han producido durante los últimos 90 segundos en todas las ocurrencias de NAT.
Total Translations	Muestra el número total de traducciones en todas las ocurrencias de NAT.
Total Translated Packets	Muestra el número total de paquetes traducidos en todas las ocurrencias de NAT.
Total Untranslated Packets	Muestra el número total de paquetes que se han omitido en todas las ocurrencias de NAT.
Refresh Communication	Haga clic para actualizar todos los datos de la ficha.
Set	Haga clic para eliminar una ocurrencia de NAT del switch después de hacer clic en el icono de papelera situado junto a la ocurrencia.

Para configurar NAT, siga uno de estos procedimientos dependiendo de su aplicación:

- Cree ocurrencias de NAT para el tráfico encaminado a través de un encaminador o un switch de capa 3

  Para conocer un ejemplo de esta aplicación, consulte la Figura 4 en la página 81.

- Cree ocurrencias de NAT para el tráfico encaminado a través de un switch de capa 2

  Para conocer un ejemplo de esta aplicación, consulte la Figura 5 en la página 81.

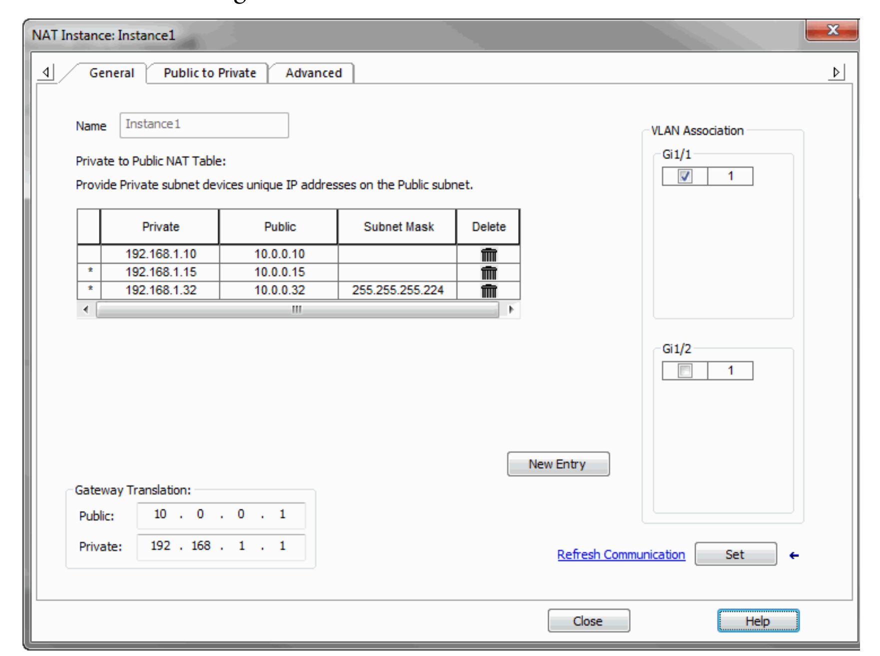
IMPORTANTE	Configure todos los roles Smartport y las VLAN antes de crear ocurrencias de NAT. Si cambia un rol Smartport o la VLAN nativa de un puerto asociado a una ocurrencia de NAT, deberá volver a asignar las VLAN a la ocurrencia de NAT.

IMPORTANTE	Como resultado del reenvío de la capa 2, las sesiones de tráfico actuales permanecen establecidas hasta que sean desconectadas manualmente. Si cambia una traducción existente, deberá desconectar manualmente todas las sesiones de tráfico asociadas antes de que la nueva traducción pueda entrar en vigor.

Cree ocurrencias de NAT para el tráfico encaminado a través de un encaminador o un switch de capa 3

Para crear una ocurrencia de NAT para el tráfico encaminado a través de un switch o encaminador de capa 3, siga estos pasos.

1. En la ficha NAT, haga clic en New Instance para abrir la ficha General del cuadro de diálogo NAT Instance.



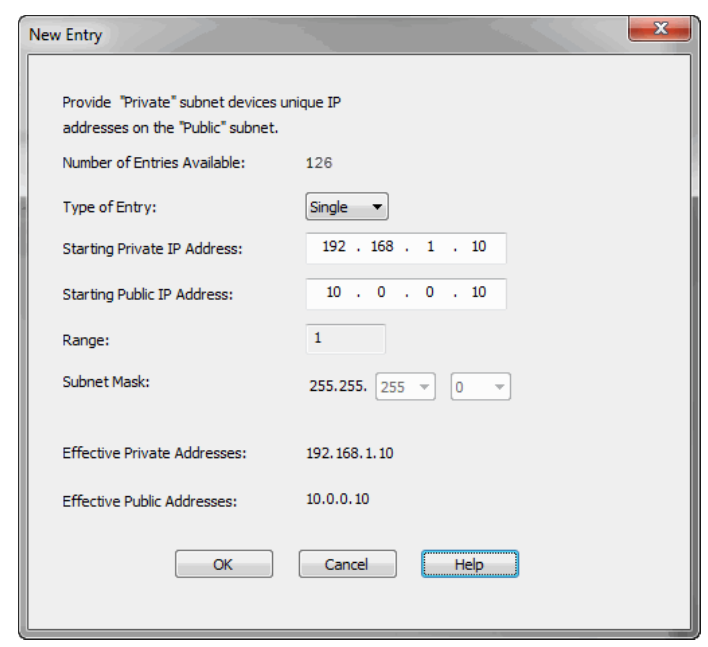
2. En el campo Name, escriba un nombre único que identifique la ocurrencia.

   El nombre de la ocurrencia no puede incluir espacios ni tener más de 32 caracteres.

3. En el área VLAN Association, marque la casilla de selección junto a cada VLAN que vaya a asignar a la ocurrencia.

   Para obtener más información acerca de las asignaciones de VLAN, consulte la página 83.

4. Haga clic en New Entry para abrir el cuadro de diálogo New Entry.



5. Realice una de las siguientes acciones:
   - Para traducir una sola dirección para un dispositivo de la subred privada que necesita comunicarse en la subred pública, rellene los siguientes campos.

Campo	Descripción
Type of Entry	Elija Single. Este es el valor predeterminado.
Starting Private IP Address	Escriba la dirección existente del dispositivo en la subred privada.
Starting Public IP Address	Escriba una dirección pública única que represente el dispositivo.
Effective Private Addresses	Muestra la dirección existente del dispositivo en la subred privada que se ha configurado para la traducción. Si está en blanco, compruebe que sean válidos los valores de los campos que aparecen encima.
Effective Public Addresses	Muestra la dirección pública única que representa el dispositivo. Si está en blanco, compruebe que sean válidos los valores de los campos que aparecen encima.

- Para traducir un rango de direcciones para dispositivos de la subred privada que necesitan comunicarse en la subred pública, rellene los siguientes campos.

Campo	Descripción
Type of Entry	Elija Range.
Starting Private IP Address	Escriba la dirección inicial existente del dispositivo en la subred privada.
Starting Public IP Address	Escriba una dirección pública inicial única que represente el dispositivo.
Range	Escriba el número de direcciones que desea incluir en el rango. Valores válidos: 1…128 Valor predeterminado = 1 **IMPORTANTE:** Cada dirección del rango cuenta como una entrada de traducción. El switch admite un máximo de 128 entradas de traducción.
Effective Private Addresses	Muestra el rango de direcciones existentes para los dispositivos de la subred privada que se han configurado para la traducción. Si está en blanco, compruebe que sean válidos los valores de los campos que aparecen encima.
Effective Public Addresses	Muestra el rango de direcciones públicas únicas que representan los dispositivos. Si está en blanco, compruebe que sean válidos los valores de los campos que aparecen encima.

- Para traducir todas las direcciones de la subred privada o una porción de la subred privada, rellene los siguientes campos.

<table>
<tr><th>Campo</th><th colspan="2">Descripción</th></tr>
<tr><td>Type of Entry</td><td colspan="2">Elija Subnet.</td></tr>
<tr><td rowspan="8">Starting Private IP Address</td><td colspan="2">Escriba la dirección inicial existente de un dispositivo en la subred privada. Esta dirección debe corresponder al tamaño de la máscara de subred que se desea traducir tal como se muestra a continuación.</td></tr>
<tr><td>Subnet Mask</td><td>Dirección inicial de subred privada</td></tr>
<tr><td>255.255.0.0</td><td>Los últimos dos octetos deben terminar en 0.
EJEMPLO: 192.168.0.0</td></tr>
<tr><td>255.255.255.0</td><td>El último octeto debe terminar en 0.
EJEMPLO: 192.168.1.0</td></tr>
<tr><td>255.255.255.128</td><td>El último octeto debe terminar en 0 o 128.
EJEMPLO: 192.168.1.0 o 192.168.1.128</td></tr>
<tr><td>255.255.255.192</td><td>El último octeto debe terminar en uno de los siguientes: 0, 64, 128, 192.
EJEMPLO: 192.168.1.64</td></tr>
<tr><td>255.255.255.224</td><td>El último octeto debe terminar en uno de los siguientes: 0, 32, 64, 96, 128, 160, 192, 224.
EJEMPLO: 192.168.1.32</td></tr>
<tr><td>255.255.255.240</td><td>El último octeto debe terminar en uno de los siguientes: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240.
EJEMPLO: 192.168.1.16</td></tr>
</table>

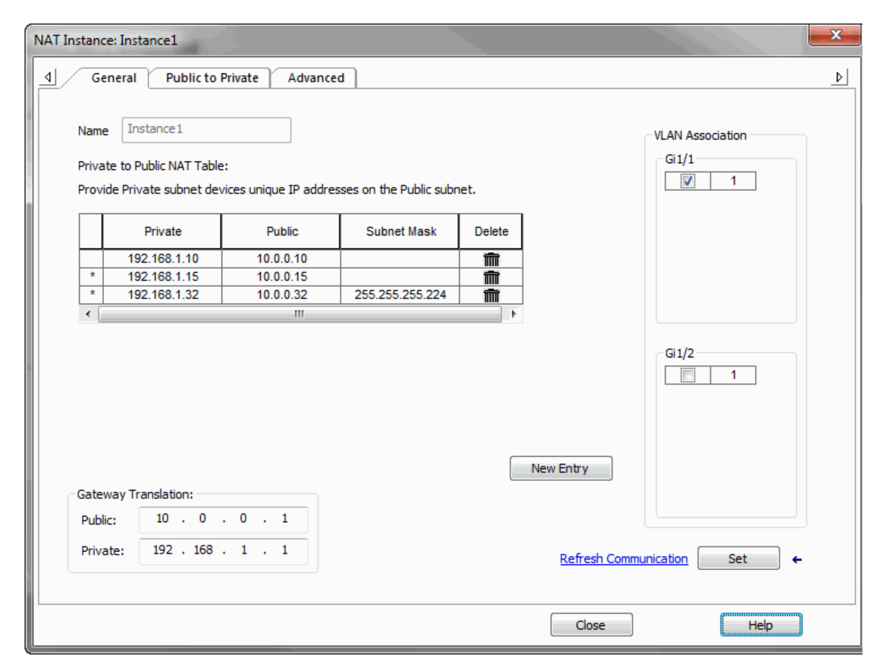
<table>
<tr><th>Campo</th><th colspan="2">Descripción</th></tr>
<tr><td rowspan="8">Starting Public IP Address</td><td colspan="2">Escriba una dirección pública inicial única que represente los dispositivos. Esta dirección debe corresponder al tamaño de la máscara de subred que se desea traducir tal como se muestra a continuación.</td></tr>
<tr><td>Subnet Mask</td><td>Dirección inicial de subred pública</td></tr>
<tr><td>255.255.0.0</td><td>Los últimos dos octetos deben terminar en 0.
EJEMPLO: 10.200.0.0</td></tr>
<tr><td>255.255.255.0</td><td>El último octeto debe terminar en 0.
EJEMPLO: 10.200.1.0</td></tr>
<tr><td>255.255.255.128</td><td>El último octeto debe terminar en 0 o 128.
EJEMPLO: 10.200.1.0 o 10.200.1.128</td></tr>
<tr><td>255.255.255.192</td><td>El último octeto debe terminar en uno de los siguientes: 0, 64, 128, 192.
EJEMPLO: 10.200.1.64</td></tr>
<tr><td>255.255.255.224</td><td>El último octeto debe terminar en uno de los siguientes: 0, 32, 64, 96, 128, 160, 192, 224.
EJEMPLO: 10.200.1.32</td></tr>
<tr><td>255.255.255.240</td><td>El último octeto debe terminar en uno de los siguientes: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240.
EJEMPLO: 10.200.1.16</td></tr>
<tr><td>Subnet Mask</td><td colspan="2">Utilice los menús desplegables para elegir la máscara de subred de las direcciones que desea traducir.
Valores válidos:
• Clase B: 255.255.0.0
• Clase C: 255.255.255.0
• Porción de clase C:
– 255.255.255.128 (proporciona 128 direcciones por entrada de traducción)
– 255.255.255.192 (proporciona 64 direcciones por entrada de traducción)
– 255.255.255.224 (proporciona 32 direcciones por entrada de traducción)
– 255.255.255.240 (proporciona 16 direcciones por entrada de traducción)</td></tr>
<tr><td>Effective Private Addresses</td><td colspan="2">Muestra el rango de direcciones existentes para los dispositivos de la subred privada que se han configurado para la traducción.
Si está en blanco, compruebe que sean válidos los valores de los campos que aparecen encima.</td></tr>
<tr><td>Effective Public Addresses</td><td colspan="2">Muestra el rango de direcciones públicas únicas que representan los dispositivos.
Si está en blanco, compruebe que sean válidos los valores de los campos que aparecen encima.</td></tr>
</table>

6. Haga clic en OK.
7. Rellene los campos de Gateway Translation para que los dispositivos de la subred pública puedan comunicarse con los dispositivos de la subred privada:
   - Public: escriba la dirección de gateway predeterminada del encaminador o switch de capa 3 conectado al puerto de vínculo ascendente del switch.
   - Private: escriba una dirección IP única que represente el encaminador o switch de capa 3 en la red privada.
8. Si desea configurar permisos de tráfico y correcciones de paquetes, continúe con Configure permisos y correcciones de tráfico en la página 198.
9. Haga clic en Set.

Cree ocurrencias de NAT para el tráfico encaminado a través de un switch de capa 2

Para crear una ocurrencia de NAT para el tráfico encaminado a través de un switch de capa 2, siga estos pasos.

1. En la ficha NAT, haga clic en New Instance para abrir el cuadro de diálogo NAT Instance.



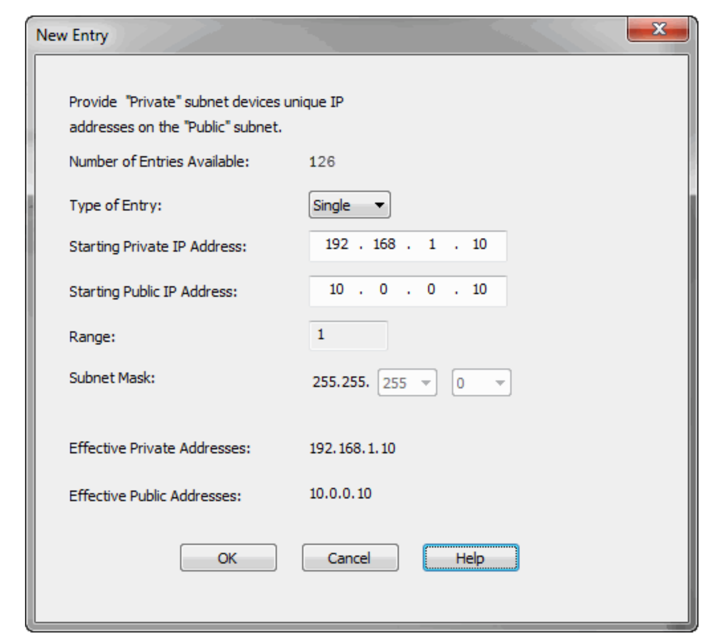
2. En el campo Name, escriba un nombre único que identifique la ocurrencia.

   El nombre de la ocurrencia no puede incluir espacios ni tener más de 32 caracteres.

3. En la lista de redes VLAN que aparece a la derecha, marque la casilla de selección junto a cada VLAN que quiera asignar a la ocurrencia.

   Para obtener más información acerca de las asignaciones de VLAN, consulte la página 83.

4. Haga clic en New Entry para abrir el cuadro de diálogo New Entry.



5. Realice una de las siguientes acciones:
   - Para traducir una sola dirección para un dispositivo de la subred privada que necesita comunicarse en la subred pública, rellene los siguientes campos.

Campo	Descripción
Type of Entry	Elija Single. Este es el valor predeterminado.
Starting Private IP Address	Escriba la dirección existente del dispositivo en la subred privada.
Starting Public IP Address	Escriba una dirección pública única que represente el dispositivo.
Effective Private Addresses	Muestra la dirección existente del dispositivo en la subred privada que se ha configurado para la traducción. Si está en blanco, compruebe que sean válidos los valores de los campos que aparecen encima.
Effective Public Addresses	Muestra la dirección pública única que representa el dispositivo. Si está en blanco, compruebe que sean válidos los valores de los campos que aparecen encima.

   - Para traducir un rango de direcciones para dispositivos de la subred privada que necesitan comunicarse en la subred pública, rellene los siguientes campos.

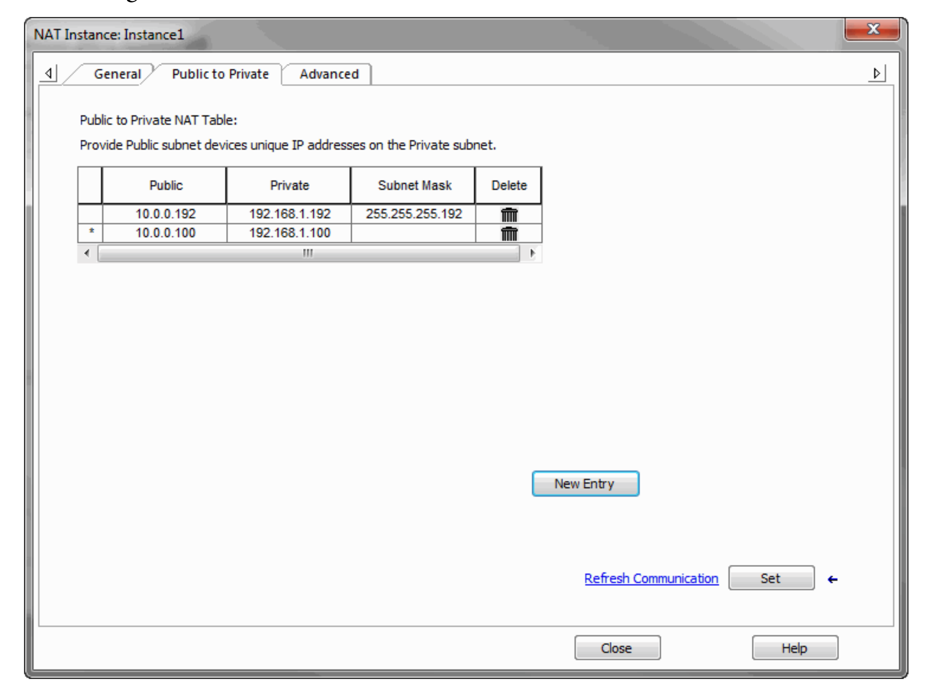
Campo	Descripción
Type of Entry	Elija Range.
Starting Private IP Address	Escriba la dirección inicial existente del dispositivo en la subred privada.
Starting Public IP Address	Escriba una dirección pública inicial única que represente los dispositivos.
Range	Escriba el número de direcciones que desea incluir en el rango. Valores válidos: 1…128 Valor predeterminado = 1 **IMPORTANTE:** Cada dirección del rango cuenta como una entrada de traducción. El switch admite un máximo de 128 entradas de traducción.
Effective Private Addresses	Muestra el rango de direcciones existentes para los dispositivos de la subred privada que se han configurado para la traducción. Si está en blanco, compruebe que sean válidos los valores de los campos que aparecen encima.
Effective Public Addresses	Muestra el rango de direcciones públicas únicas que representan los dispositivos. Si está en blanco, compruebe que sean válidos los valores de los campos que aparecen encima.

- Para traducir todas las direcciones de la subred privada o una porción de la subred privada, rellene los campos tal como se describe en la siguiente tabla.

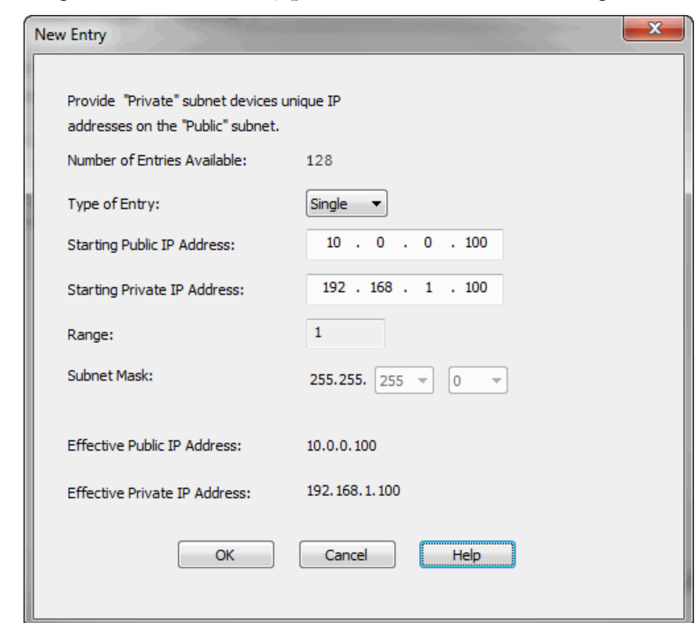
<table>
<tr><th>Campo</th><th>Descripción</th></tr>
<tr><td>Type of Entry</td><td>Elija Subnet.</td></tr>
<tr><td>Starting Private IP Address</td><td>Escriba la dirección inicial existente de un dispositivo en la subred privada. Esta dirección debe corresponder al tamaño de la máscara de subred que se desea traducir tal como se muestra a continuación.
<table>
<tr><th>Máscara de subred</th><th>Dirección inicial de subred privada</th></tr>
<tr><td>255.255.0.0</td><td>Los últimos dos octetos deben terminar en 0.
EJEMPLO: 192.168.0.0</td></tr>
<tr><td>255.255.255.0</td><td>El último octeto debe terminar en 0.
EJEMPLO: 192.168.1.0</td></tr>
<tr><td>255.255.255.128</td><td>El último octeto debe terminar en 0 o 128.
EJEMPLO: 192.168.1.0 o 192.168.1.128</td></tr>
<tr><td>255.255.255.192</td><td>El último octeto debe terminar en uno de los siguientes: 0, 64, 128, 192.
EJEMPLO: 192.168.1.64</td></tr>
<tr><td>255.255.255.224</td><td>El último octeto debe terminar en uno de los siguientes: 0, 32, 64, 96, 128, 160, 192, 224.
EJEMPLO: 192.168.1.32</td></tr>
<tr><td>255.255.255.240</td><td>El último octeto debe terminar en uno de los siguientes: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240.
EJEMPLO: 192.168.1.16</td></tr>
</table></td></tr>
<tr><td>Starting Public IP Address</td><td>Escriba una dirección pública inicial única que represente los dispositivos. Esta dirección debe corresponder al tamaño de la máscara de subred que se desea traducir tal como se muestra a continuación.
<table>
<tr><th>Máscara de subred</th><th>Dirección inicial de subred pública</th></tr>
<tr><td>255.255.0.0</td><td>Los últimos dos octetos deben terminar en 0.
EJEMPLO: 10.200.0.0</td></tr>
<tr><td>255.255.255.0</td><td>El último octeto debe terminar en 0.
EJEMPLO: 10.200.1.0</td></tr>
<tr><td>255.255.255.128</td><td>El último octeto debe terminar en 0 o 128.
EJEMPLO: 10.200.1.0 o 10.200.1.128</td></tr>
<tr><td>255.255.255.192</td><td>El último octeto debe terminar en uno de los siguientes: 0, 64, 128, 192.
EJEMPLO: 10.200.1.64</td></tr>
<tr><td>255.255.255.224</td><td>El último octeto debe terminar en uno de los siguientes: 0, 32, 64, 96, 128, 160, 192, 224.
EJEMPLO: 10.200.1.32</td></tr>
<tr><td>255.255.255.240</td><td>El último octeto debe terminar en uno de los siguientes: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240.
EJEMPLO: 10.200.1.16</td></tr>
</table></td></tr>
</table>

Campo	Descripción
Subnet Mask	Utilice los menús desplegables para elegir la máscara de subred de las direcciones que desea traducir. Valores válidos: • Clase B: 255.255.0.0 • Clase C: 255.255.255.0 • Porción de clase C: – 255.255.255.128 (proporciona 128 direcciones por entrada de traducción) – 255.255.255.192 (proporciona 64 direcciones por entrada de traducción) – 255.255.255.224 (proporciona 32 direcciones por entrada de traducción) – 255.255.255.240 (proporciona 16 direcciones por entrada de traducción)
Effective Private Addresses	Muestra el rango de direcciones existentes para los dispositivos de la subred privada que se han configurado para la traducción. Si está en blanco, compruebe que sean válidos los valores de los campos que aparecen encima.
Effective Public Addresses	Muestra el rango de direcciones públicas únicas que representan los dispositivos. Si está en blanco, compruebe que sean válidos los valores de los campos que aparecen encima.

6. Haga clic en OK.
7. Haga clic en la ficha Public to Private.



8. Haga clic en New Entry para abrir el cuadro de diálogo New Entry.



9. Realice una de las siguientes acciones:
   - Para traducir una sola dirección para un dispositivo de la subred pública que necesita comunicarse en la subred privada, rellene los siguientes campos.

Campo	Descripción
Type of Entry	Elija Single. Este es el valor predeterminado.
Starting Public IP Address	Escriba la dirección existente del dispositivo en la subred pública.
Starting Private IP Address	Escriba una dirección privada única que represente el dispositivo.
Effective Public Addresses	Muestra la dirección existente del dispositivo en la subred pública que se ha configurado para la traducción. Si está en blanco, compruebe que sean válidos los valores de los campos que aparecen encima.
Effective Private Addresses	Muestra la dirección privada única que representa el dispositivo. Si está en blanco, compruebe que sean válidos los valores de los campos que aparecen encima.

   - Para traducir un rango de direcciones para dispositivos de la subred pública que necesitan comunicarse en la subred privada, rellene los siguientes campos.

Campo	Descripción
Type of Entry	Elija Range.
Starting Public IP Address	Escriba la dirección inicial existente del dispositivo en la subred pública.
Starting Private IP Address	Escriba una dirección privada inicial única que represente los dispositivos.
Range	Escriba el número de direcciones que desea incluir en el rango. Valores válidos: 1…128 Valor predeterminado = 1 **IMPORTANTE:** Cada dirección del rango cuenta como una entrada de traducción. El switch admite un máximo de 128 entradas de traducción.
Effective Public Addresses	Muestra el rango de direcciones existentes para los dispositivos de la subred pública que se han configurado para la traducción. Si está en blanco, compruebe que sean válidos los valores de los campos que aparecen encima.
Effective Private Addresses	Muestra el rango de direcciones privadas únicas que representan los dispositivos. Si está en blanco, compruebe que sean válidos los valores de los campos que aparecen encima.

- Para traducir todas las direcciones de la subred privada o una porción de la subred privada, rellene los campos tal como se describe en la siguiente tabla.

<table>
<tr><th>Campo</th><th colspan="2">Descripción</th></tr>
<tr><td>Type of Entry</td><td colspan="2">Elija Subnet.</td></tr>
<tr><td rowspan="8">Starting Public IP Address</td><td colspan="2">Escriba la dirección inicial existente de un dispositivo en la subred pública. Esta dirección debe corresponder al tamaño de la máscara de subred que se desea traducir tal como se muestra a continuación.</td></tr>
<tr><td>Máscara de subred</td><td>Dirección inicial de subred pública</td></tr>
<tr><td>255.255.0.0</td><td>Los últimos dos octetos deben terminar en 0.
EJEMPLO: 10.200.0.0</td></tr>
<tr><td>255.255.255.0</td><td>El último octeto debe terminar en 0.
EJEMPLO: 10.200.1.0</td></tr>
<tr><td>255.255.255.128</td><td>El último octeto debe terminar en 0 o 128.
EJEMPLO: 10.200.1.0 o 10.200.1.128</td></tr>
<tr><td>255.255.255.192</td><td>El último octeto debe terminar en uno de los siguientes: 0, 64, 128, 192.
EJEMPLO: 10.200.1.64</td></tr>
<tr><td>255.255.255.224</td><td>El último octeto debe terminar en uno de los siguientes: 0, 32, 64, 96, 128, 160, 192, 224.
EJEMPLO: 10.200.1.32</td></tr>
<tr><td>255.255.255.240</td><td>El último octeto debe terminar en uno de los siguientes: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240.
EJEMPLO: 10.200.1.16</td></tr>
<tr><td rowspan="8">Starting Private IP Address</td><td colspan="2">Escriba una dirección privada inicial única que represente los dispositivos. Esta dirección debe corresponder al tamaño de la máscara de subred que se desea traducir tal como se muestra a continuación.</td></tr>
<tr><td>Máscara de subred</td><td>Dirección inicial de subred privada</td></tr>
<tr><td>255.255.0.0</td><td>Los últimos dos octetos deben terminar en 0.
EJEMPLO: 192.168.0.0</td></tr>
<tr><td>255.255.255.0</td><td>El último octeto debe terminar en 0.
EJEMPLO: 192.168.1.0</td></tr>
<tr><td>255.255.255.128</td><td>El último octeto debe terminar en 0 o 128.
EJEMPLO: 192.168.1.0 o 192.168.1.128</td></tr>
<tr><td>255.255.255.192</td><td>El último octeto debe terminar en uno de los siguientes: 0, 64, 128, 192.
EJEMPLO: 192.168.1.64</td></tr>
<tr><td>255.255.255.224</td><td>El último octeto debe terminar en uno de los siguientes: 0, 32, 64, 96, 128, 160, 192, 224.
EJEMPLO: 192.168.1.32</td></tr>
<tr><td>255.255.255.240</td><td>El último octeto debe terminar en uno de los siguientes: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240.
EJEMPLO: 192.168.1.16</td></tr>
</table>

Campo	Descripción
Subnet Mask	Utilice los menús desplegables para elegir la máscara de subred de las direcciones que desea traducir. Valores válidos: • Clase B: 255.255.0.0 • Clase C: 255.255.255.0 • Porción de clase C: – 255.255.255.128 (proporciona 128 direcciones por entrada de traducción) – 255.255.255.192 (proporciona 64 direcciones por entrada de traducción) – 255.255.255.224 (proporciona 32 direcciones por entrada de traducción) – 255.255.255.240 (proporciona 16 direcciones por entrada de traducción)
Effective Public Addresses	Muestra el rango de direcciones existentes para los dispositivos de la subred pública que se han configurado para la traducción. Si está en blanco, compruebe que sean válidos los valores de los campos que aparecen encima.
Effective Private Addresses	Muestra el rango de direcciones privadas únicas que representan los dispositivos. Si está en blanco, compruebe que sean válidos los valores de los campos que aparecen encima.

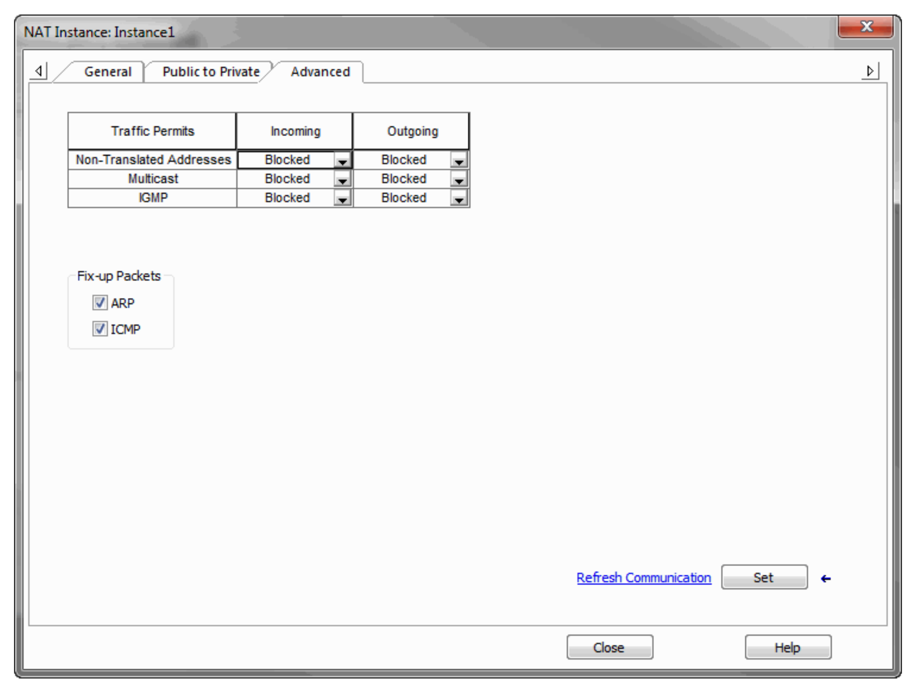
10. Haga clic en OK.
11. (Opcional). Si desea configurar permisos de tráfico y correcciones de paquetes, continúe con Configure permisos y correcciones de tráfico en la página 198.
12. Haga clic en Set.

Configure permisos y correcciones de tráfico

Tenga cuidado al configurar los permisos y las correcciones de tráfico.
Le recomendamos que utilice los valores predeterminados.

Para configurar permisos de tráfico o correcciones de paquetes, siga estos pasos.

1. Haga clic en la ficha Advanced.



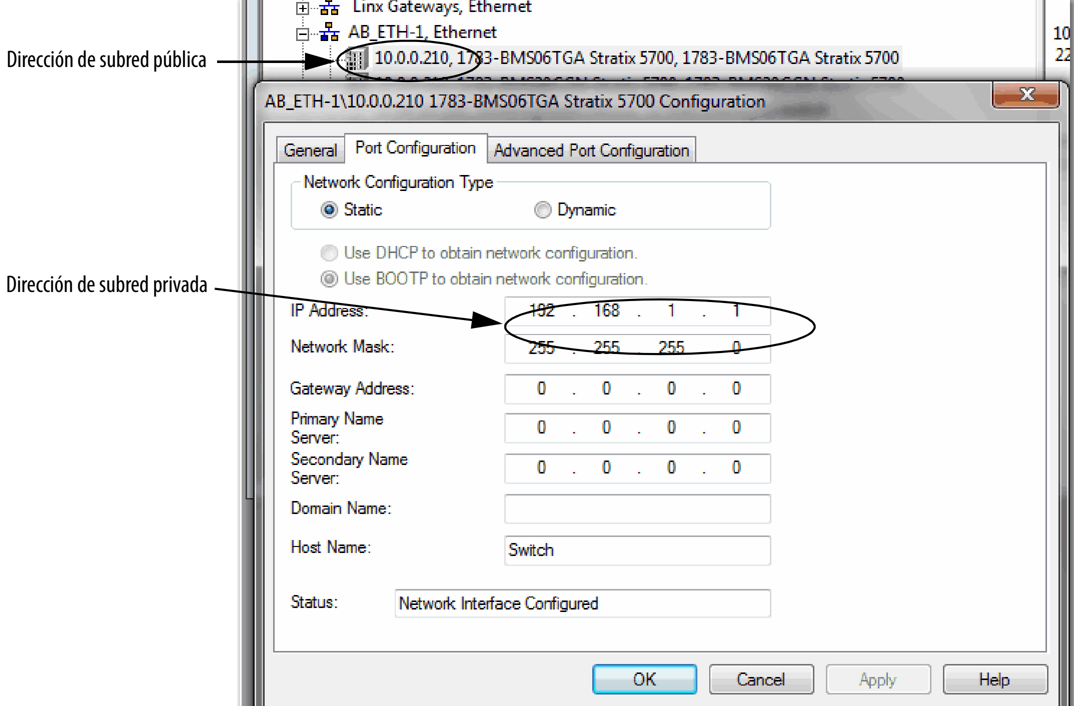
2. En la cuadrícula Traffic Permits, elija una de estas opciones para los paquetes entrantes y salientes que no maneje NAT:
   - Pass-Through: permite que los paquetes atraviesen el límite de NAT.
   - Blocked: borra los paquetes.
3. En el área Fix-up Packets, marque o desmarque las casillas de selección para habilitar o inhabilitar las correcciones de protocolo para ARP e ICMP.

   De manera predeterminada, las correcciones están habilitadas para ARP e ICMP.

Vea traducciones de direcciones en el software RSLinx

El driver Ethernet del software RSLinx admite dispositivos con traducciones de direcciones. Si la dirección de un dispositivo está configurada para traducción, su dirección de subred pública aparecerá en el cuadro de diálogo principal del software RSLinx. No obstante, su dirección de subred privada aparecerá en las propiedades de configuración del dispositivo.

Figura 9 - Direcciones de subredes públicas y privadas en el software RSLinx

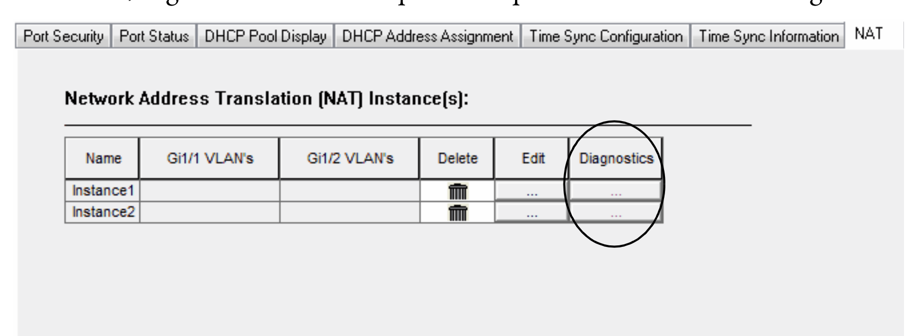


Diagnósticos de NAT

Para cada ocurrencia de NAT, puede monitorear los siguientes diagnósticos:

- Diagnósticos para traducciones privadas y públicas
- Diagnósticos solo para traducciones privadas
- Diagnósticos solo para traducciones públicas

Para obtener acceso a los diagnósticos correspondientes a una ocurrencia, en la ficha NAT, haga clic en el botón de puntos suspensivos de la columna Diagnostics.



El cuadro de diálogo NAT Diagnostics muestra los diagnósticos de la ocurrencia seleccionada.

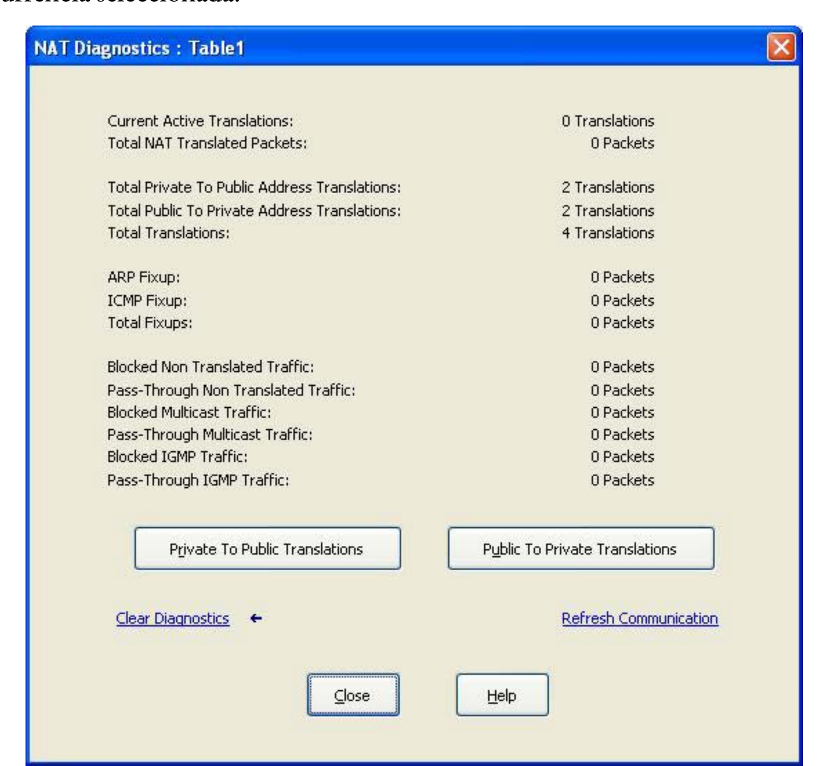


Tabla 42 - Diagnósticos de NAT por ocurrencia

Campo	Descripción
Current Active Translations	Muestra el número de traducciones que se han producido durante los últimos 90 segundos en todas las ocurrencias de NAT.
Total NAT Translated Packets	Muestra el número total de paquetes que se han traducido para esta ocurrencia.
Total Private to Public Address Translations	Muestra el número total de traducciones de privada a pública para esta ocurrencia.
Total Public to Private Address Translations	Muestra el número total de traducciones de pública a privada para esta ocurrencia.
ARP Fixup	Muestra el número de paquetes ARP que se han corregido para esta ocurrencia.
ICMP Fixup	Muestra el número de paquetes ICMP que se han corregido para esta ocurrencia.
Total Fixups	Muestra el número de paquetes ARP e ICMP que se han corregido para esta ocurrencia.
Incoming Non Translated Traffic (Pass-Through)	Muestra el número de paquetes entrantes con tráfico no traducido que NAT ha dejado pasar para esta ocurrencia.
Outgoing Non Translated Traffic (Blocked)	Muestra el número de paquetes salientes con tráfico no traducido que NAT ha bloqueado para esta ocurrencia.
Incoming Multicast Traffic (Blocked)	Muestra el número de paquetes entrantes con tráfico de multidifusión que NAT ha bloqueado para esta ocurrencia.
Outgoing Multicast Traffic (Pass-Through)	Muestra el número de paquetes salientes de tráfico de multidifusión que NAT ha dejado pasar para esta ocurrencia.
Incoming IGMP Traffic (Blocked)	Muestra el número de paquetes entrantes con tráfico IGMP que NAT ha bloqueado para esta ocurrencia.
Outgoing IGMP Traffic (Blocked)	Muestra el número de paquetes salientes con tráfico IGMP que NAT ha bloqueado para esta ocurrencia.
Private to Public Translations	Haga clic para ver los diagnósticos de traducción privada a pública para la ocurrencia. Consulte Diagnósticos de traducción privada a pública en la página 202.
Public to Private Translations	Haga clic para ver los diagnósticos de traducción privada a pública para la ocurrencia. Consulte Diagnósticos de traducción pública a privada en la página 203.
Refresh Communication	Haga clic para actualizar todos los diagnósticos para esta ocurrencia.

Diagnósticos de traducción privada a pública

Mediante el cuadro de diálogo Private to Public Translations de una ocurrencia, puede ver una lista de direcciones IP que NAT ha cambiado durante los últimos 90 segundos.

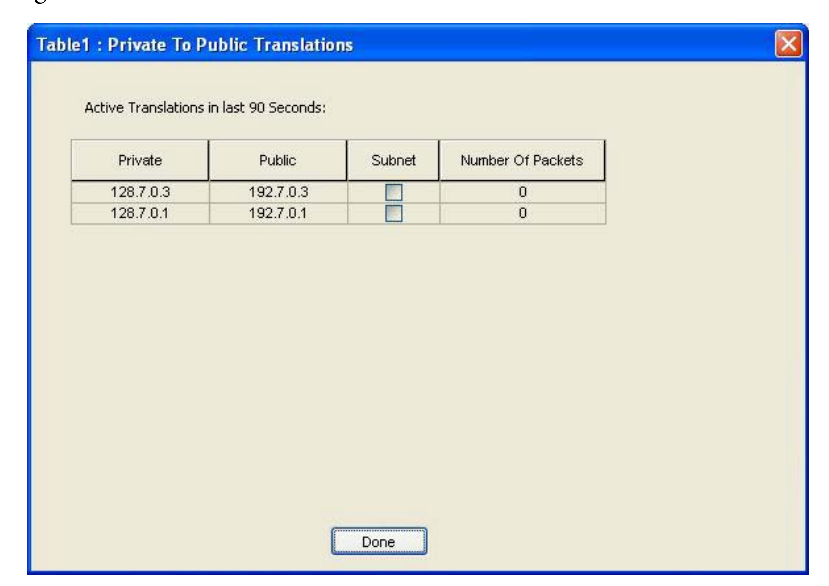


Tabla 43 - Diagnósticos de traducción privada a pública

Campo	Descripción
Private	Muestra la dirección existente de un dispositivo en la subred privada.
Public	Muestra una dirección pública única que representa el dispositivo correspondiente en la subred privada.
Subnet	Indica si la traducción forma parte de un tipo de entrada Subnet.
Number of Packets	Muestra el número de paquetes que contiene la traducción.

Diagnósticos de traducción pública a privada

Mediante el cuadro de diálogo Public to Private Translations de una ocurrencia, puede ver una lista de direcciones IP que NAT ha cambiado durante los últimos 90 segundos.

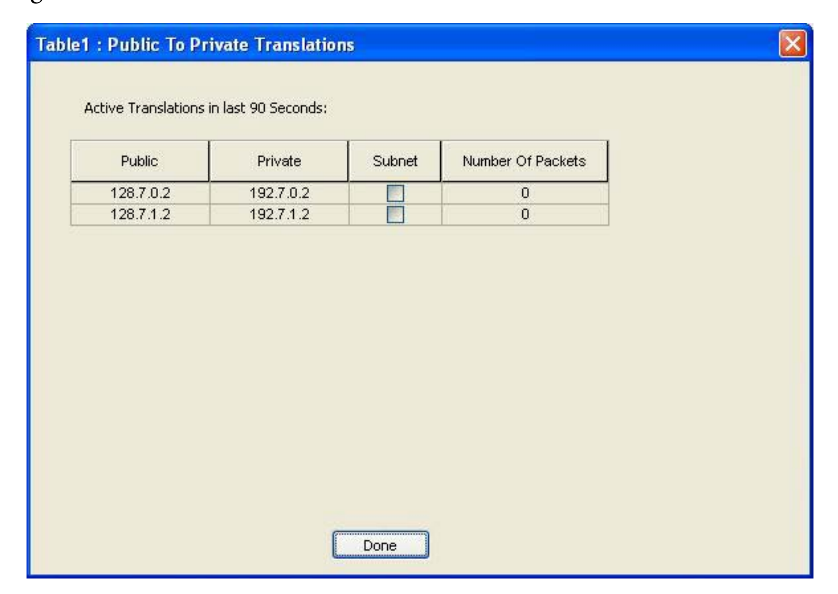


Tabla 44 - Diagnósticos de traducción pública a privada

Campo	Descripción
Public	Muestra la dirección IP única en la subred pública que representa la dirección IP correspondiente en la subred privada.
Private	Muestra la dirección IP en la subred privada que se cambió a una dirección IP única en la subred pública.
Subnet	Indica si la traducción forma parte de un tipo de entrada Subnet.
Number of Packets	Muestra el número de paquetes que contiene la traducción.

Sincronización flash SD

Puede sincronizar la tarjeta SD, ya sea con el archivo de configuración, o bien con la imagen completa.

IMPORTANTE	Puede sobrescribir la configuración si realiza la sincronización en la dirección incorrecta.

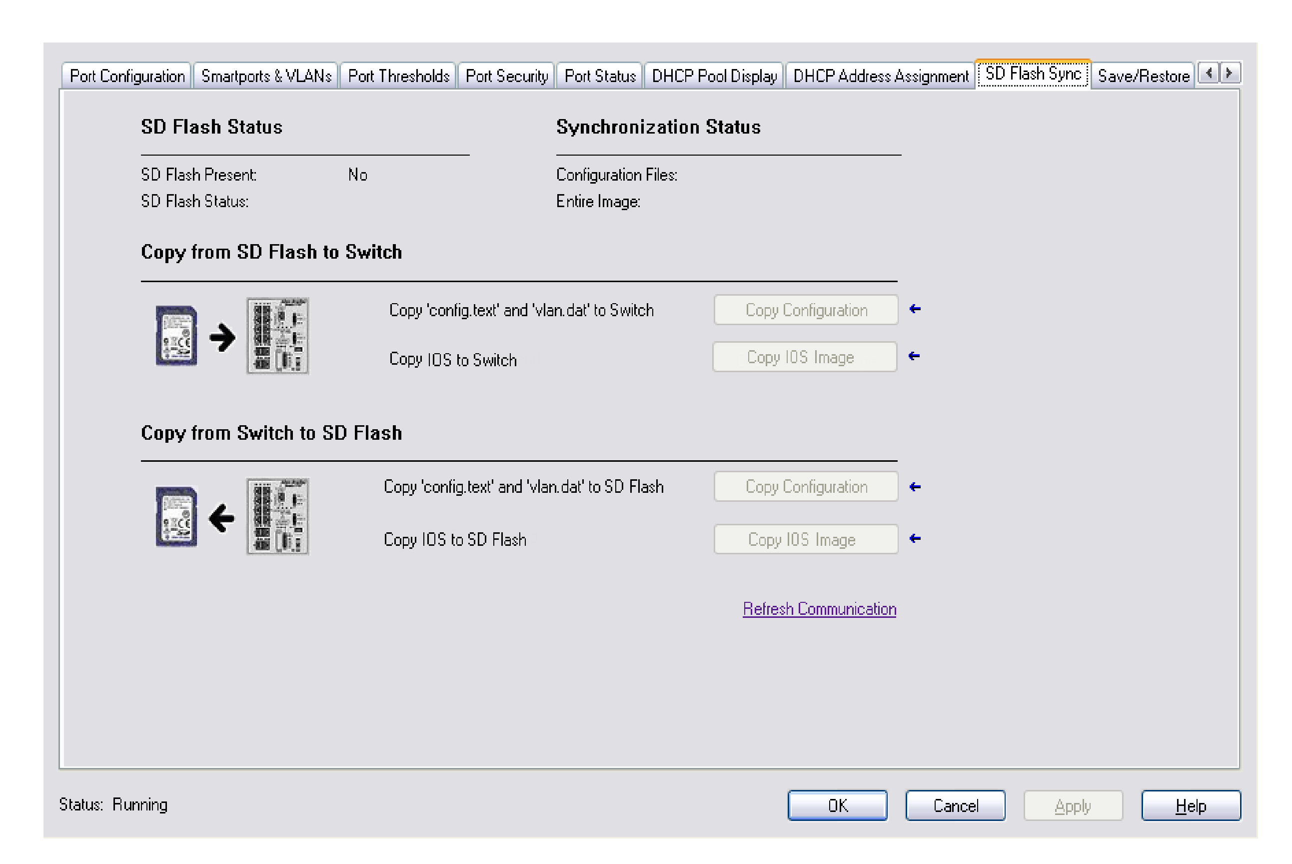


Tabla 45 - Campos de la ficha SD Flash Sync

Campo	Descripción
SD Flash Status	Indica si se ha insertado una tarjeta SD y el estado de la tarjeta.
Synchronization Status	Indica si los archivos de configuración y el IOS están sincronizados o no.
Copy from SD Flash to Switch	Elija una de estas opciones: • Copy Configuration • Copy IOS Image
Copy from Switch to SD Flash	Elija una de estas opciones: • Copy Configuration • Copy IOS Image

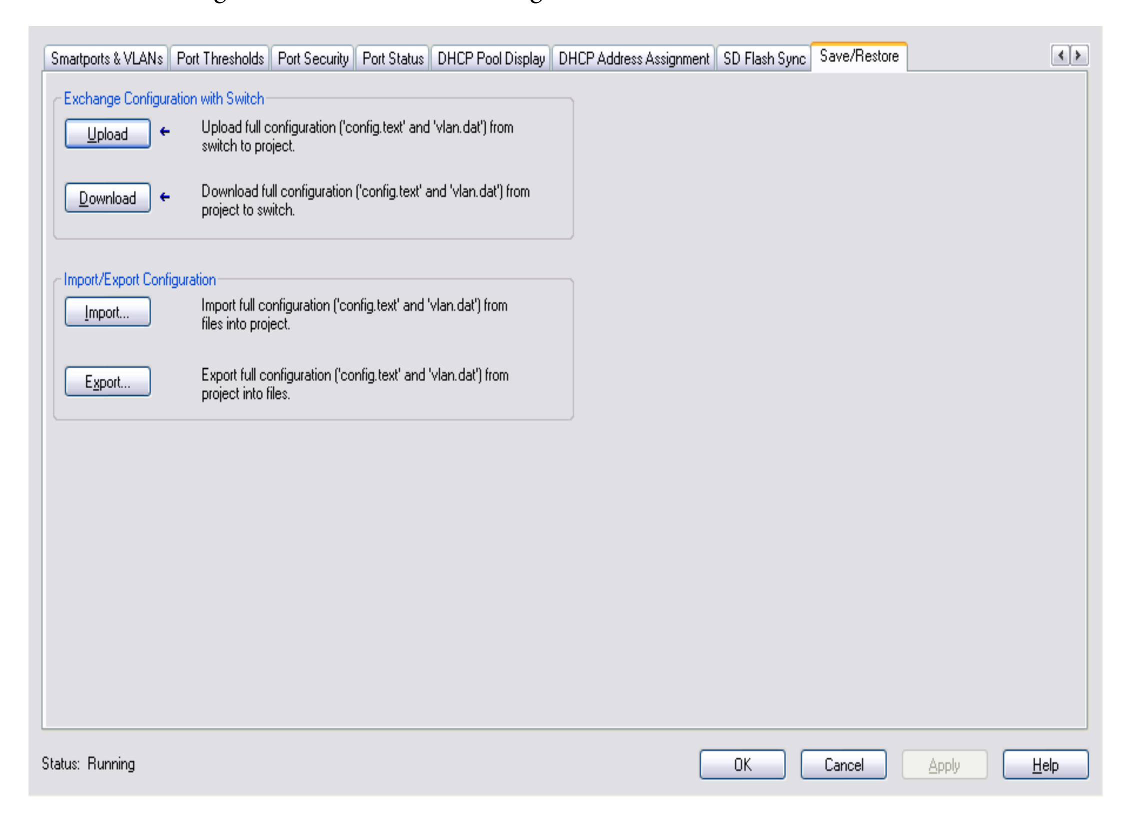
Guarde y restaure la configuración del switch

Utilice esta ficha para lo siguiente:

- Guardar la configuración del switch en un archivo para archivarla
- Restaurar una configuración del switch almacenada localmente en la computadora o en el proyecto de aplicación de Logix Designer.

Debe estar en línea para guardar y restaurar archivos de configuración. La mayoría de los ajustes aparecen atenuados cuando el switch está fuera de línea.

Debe estar preparado para escribir una contraseña válida del switch si desea guardar o restaurar una configuración del switch.



La configuración del switch consta de estos dos archivos:

- Archivo de texto con los parámetros de configuración
- Archivo binario con la información de VLAN

Una vez que se carga la configuración del switch al archivo de proyecto de la aplicación Logix Designer, se puede exportar la configuración del switch como archivos informáticos mediante el botón Export.

Puede importar al proyecto una configuración del switch desde los archivos adecuados de su computadora mediante el botón del AOP del switch. A continuación, puede descargar la configuración al switch mediante el botón Download del AOP. Consulte Guarde y restaure la configuración del switch en la página 205 para obtener más información acerca de la característica Save and Restore.

Notas:

Resolución de problemas del switch

Este capítulo le ayuda a resolver problemas relacionados con los switches Stratix 5700, así como a realizar funciones comunes como restablecer el switch.

Para obtener más ayuda en torno a la resolución de problemas, consulte lo siguiente:

- Diagnostique problemas de cableado en la página 152
- Vea mensajes de registro del sistema en la página 153

Verifique la inicialización rápida

Los fallos de inicialización rápida pueden ser fatales para el switch. Comuníquese con el representante de Rockwell Automation si el switch no completa correctamente la inicialización rápida. Puede inhabilitar la inicialización rápida y ejecutar una autoprueba de encendido (POST) mediante la CLI.

Problemas con la dirección IP

Hay algunas sugerencias básicas para la resolución de problemas relacionados con la dirección IP del switch.

Problema	Resolución
No se recibe la dirección IP del servidor DHCP	Si el switch no recibe una dirección IP de un dispositivo flujo arriba que funcione como servidor DHCP, asegúrese de que el dispositivo flujo arriba esté funcionando como servidor DHCP y siga de nuevo los procedimientos de configuración del switch descritos en el capítulo1, Acerca de los switches .
El switch tiene una dirección IP errónea	Si el switch está instalado en la red pero usted no puede obtener acceso al switch porque tiene una dirección IP errónea, asigne una nueva dirección IP al switch. Consulte Acceso al modo administrado directo en la página 209 para asignar la dirección IP y, a continuación, actualice la dirección IP del switch en la ventana Express Setup del administrador de dispositivos.

Problemas de la interface web del administrador de dispositivos

Hay algunas sugerencias básicas para la resolución de problemas relacionados con la interface web del administrador de dispositivos.

Problema	Resolución
La interface web del administrador de dispositivos no aparece en pantalla	Si no puede visualizar la interface web del administrador de dispositivos desde su computadora personal, asegúrese de que ha introducido la dirección IP correcta del switch en su navegador. Si ha introducido la dirección IP correcta del switch en el navegador, asegúrese de que el switch y su computadora personal estén en la misma red o subred: • Por ejemplo, si la dirección IP del switch es 172.20.20.85 y la dirección IP de su computadora personal es 172.20.20.84, ambos dispositivos están en la misma red. • Por ejemplo, si la dirección IP del switch es 172.20.20.85 y la dirección IP de su computadora personal es 10.0.0.2, los dispositivos están en redes distintas y no se podrán comunicar directamente sin un encaminador. Debe cambiar la dirección IP del switch o cambiar la dirección IP de la computadora personal. • Si el problema persiste, siga el procedimiento descrito en la sección Acceso al modo administrado directo en la página 209 y, a continuación, actualice los ajustes de la red del switch en la ventana Express Setup del administrador de dispositivos. • Si el problema aún persiste, siga el procedimiento que aparece en la sección Recupere el firmware del switch y restaure los ajustes predeterminados establecidos en fábrica en la página 211.
La interface web del administrador de dispositivos no funciona correctamente	Si la interface web del administrador de dispositivos no funciona correctamente (por ejemplo, el administrador de dispositivos no responde), siga el procedimiento descrito en la sección Acceso al modo administrado directo en la página 209, y, a continuación, actualice los ajustes de la red del switch en la ventana Express Setup de la interface web del administrador de dispositivos. Si el problema aún persiste, siga el procedimiento descrito en la sección Recupere el firmware del switch y restaure los ajustes predeterminados establecidos en fábrica en la página 211.
La interface web del administrador de dispositivos no está accesible a través de la red	Si no puede obtener acceso al administrador de dispositivos de forma remota desde un navegador web, siga el procedimiento descrito en la sección Acceso al modo administrado directo en la página 209.

Rendimiento del switch

Hay algunas sugerencias básicas para la resolución de problemas relacionados con el rendimiento del switch.

Problema	Resolución
Velocidad, modo dúplex y autonegociación	Si las estadísticas del puerto muestran una gran cantidad de errores de alineación, errores de secuencia de comprobación de trama (FCS) o errores por colisiones tardías, esto puede indicar una desigualdad de velocidad o de modo dúplex. Habitualmente se produce un problema con la velocidad y el modo dúplex cuando existe desigualdad de los ajustes de modo dúplex entre dos switches, entre un switch y un encaminador, o entre el switch y una estación de trabajo o servidor. Esto puede ocurrir cuando se configura manualmente la velocidad y el modo dúplex, o por problemas de autonegociación entre los dos dispositivos. Se produce una desigualdad en estas circunstancias: • Un parámetro de velocidad o modo dúplex establecido manualmente es diferente del parámetro de velocidad o modo dúplex establecido manualmente en el puerto conectado. • Un puerto se establece en autonegociación y el puerto conectado se establece en full-duplex sin autonegociación. Para maximizar el rendimiento del switch y estar seguro de un vínculo, siga una de estas pautas cuando cambie los ajustes de velocidad y modo dúplex: • Deje que ambos puertos autonegocien la velocidad y el modo dúplex. • Establezca manualmente los mismos parámetros de velocidad y modo dúplex para los puertos en ambos extremos de la conexión en los mismos valores. • Si un dispositivo remoto no autonegocia, configure los ajustes de modo dúplex en los dos puertos con los mismos valores. El parámetro de velocidad se puede autoajustar incluso si el puerto conectado no autonegocia.
Autonegociación y tarjetas de interface de red (NIC)	A veces se producen problemas entre el switch y las tarjetas de interface de red (NIC) de terceros. De manera predeterminada, los puertos del switch y las interfaces están establecidos en autonegociación. Habitualmente dispositivos como computadoras portátiles y otros dispositivos se establecen también en autonegociación, aunque a veces se producen problemas con la autonegociación. Para tratar de resolver problemas de autonegociación, establezca manualmente ambos lados de la conexión. Si así no se resuelve el problema, podría haber un problema con el firmware o el software en su NIC. Puede solucionarlo actualizando el driver de la NIC con el más reciente firmware o software disponible del fabricante.
Distancia de cableado	Si las estadísticas del puerto muestran excesivos errores de FCS, errores por colisiones tardías o errores de alineación, verifique que la distancia del cable desde el switch al dispositivo conectado cumpla las pautas recomendadas.

Acceso al modo administrado directo

Puede abrir la interface web del administrador de dispositivos y administrar el switch a través de una conexión física entre uno de los puertos del switch y su computadora personal. Este tipo de conexión de administración se denomina modo administrado directo. Este modo se utiliza normalmente para establecer la conexión con el switch mediante la interface web del administrador de dispositivos cuando no se conoce la dirección IP del switch.

Antes de que pueda obtener acceso al modo administrado directo, debe asegurarse de lo siguiente:

- Deberá tener acceso físico al switch.
- Asegúrese de que se haya habilitado al menos un puerto del switch y de que no esté conectado a un dispositivo.

Para obtener acceso al modo administrado directo, siga estos pasos.

1. Pulse el botón Express Setup hasta que el indicador de estado Setup parpadee de color verde y el indicador de estado de un puerto de vínculo descendente del switch parpadee de color verde.

   El puerto que tenga el indicador de estado parpadeante de color verde se designa como el puerto de modo administrado directo. Este puerto se determina del modo siguiente:

   - Si ninguno de los puertos de vínculo descendente está conectado a dispositivos o si hay varios puertos de vínculo descendente conectados a dispositivos, el primer puerto de vínculo descendente disponible se selecciona como puerto de modo administrado directo.
   - Si solo hay un puerto de vínculo descendente conectado a un dispositivo, ese puerto se selecciona como puerto de modo administrado directo.

   Si no hay ningún puerto de vínculo descendente disponible al cual conectar su computadora personal, desconecte un dispositivo de uno de los puertos de vínculo descendente y pulse el botón Setup de nuevo hasta que el indicador de estado Setup y el indicador de estado del puerto parpadeen de color verde.

2. Utilice un cable Ethernet de categoría 5 para conectar su computadora personal al puerto del switch que tiene el indicador de estado del puerto parpadeante.

3. Espere hasta que los indicadores de estado del puerto en el switch y en su computadora personal estén de color verde fijo.

   Los indicadores de estado del puerto en color verde fijo indican que se han conectado correctamente los dos dispositivos.

4. Abra un navegador web en su computadora personal.

   Aparecerá una indicación para introducir la contraseña, seguida de la página de la interface web del administrador de dispositivos.

   Si no aparece la interface web del administrador de dispositivos, asegúrese de que estén inhabilitados los bloqueadores de ventanas emergentes o los ajustes del proxy en el software de su navegador y los clientes inalámbricos que se ejecutan en su computadora personal.

   Si la interface web del administrador de dispositivos sigue sin aparecer, introduzca un URL en su navegador, como http://www.rockwellautomation.com. El navegador lo redireccionará a la interface web del administrador de dispositivos.

Reinicie o restablezca el switch

Si no puede resolver un problema mediante la reconfiguración de una característica, el reinicio o restablecimiento del switch puede solucionarle el problema o ayudarle a eliminar las causas probables. Si el problema persiste después de restablecer el switch a sus ajustes predeterminados, es poco probable que el switch sea la causa del problema.

Opción	Descripción
Reiniciar	Esta opción reinicia el switch sin apagar la alimentación. El switch conserva sus ajustes de configuración guardados durante el proceso de reinicio. No obstante, la interface web del administrador de dispositivos no se encuentra disponible durante el proceso. Cuando se completa el proceso, el switch muestra la interface web del administrador de dispositivos. **IMPORTANTE:** Al reiniciar el switch se interrumpe la conectividad de los dispositivos con la red.
Restablecer el switch a los ajustes predeterminados establecidos en fábrica	Esta opción restablece el switch, borra los ajustes de configuración actuales, devuelve los ajustes predeterminados establecidos en fábrica y finalmente reinicia el switch. **ATENCIÓN:** Al restablecer el switch se borran todos los ajustes personalizados del switch, incluida la dirección IP, y devuelve al switch los ajustes predeterminados establecidos en fábrica. Se conserva la misma imagen de software. Debe reconfigurar los ajustes básicos del switch. Consulte Configure inicialmente el switch con Express Setup en la página 50. **ATENCIÓN:** Al restablecer el switch se interrumpe la conectividad de los dispositivos con la red.

IMPORTANTE	Al reiniciar o restablecer el switch se interrumpe la conectividad de los dispositivos con la red.

Reinicie el switch desde la interface web del administrador de dispositivos

Desde la interface web del administrador de dispositivos, en el cuadro de diálogo Restart/Reset, haga clic en Restart the Switch.

Esta opción reinicia el switch sin apagar la alimentación. La interface web del administrador de dispositivos no se encuentra disponible durante el proceso de reinicio. Cuando se completa el proceso, el switch muestra la interface web del administrador de dispositivos.

Si no conoce la dirección IP del switch, siga el procedimiento descrito en la sección Acceso al modo administrado directo en la página 209 para obtener acceso al modo administrado directo.

Reinicie el switch desde la aplicación Logix Designer

Desde el cuadro de diálogo Module Properties dentro de la aplicación Logix Designer, realice lo siguiente.

1. Haga clic en la ficha Module Info.
2. Haga clic en Reset Module.

   Aparecerá una indicación para introducir la contraseña.
3. Introduzca su contraseña y haga clic en Enter.

Restablezca el switch a los ajustes predeterminados establecidos en fábrica



ATENCIÓN: Al restablecer el switch se borran todos los ajustes personalizados del switch, incluida la dirección IP, y devuelve al switch sus ajustes predeterminados establecidos en fábrica. Se conserva la misma imagen de software. Para administrar el switch o mostrar el administrador de dispositivos, debe reconfigurar los ajustes básicos del switch (según se describe en el capítulo 4, Administración del switch mediante la interface web del administrador de dispositivos) y utilizar la nueva dirección IP.

IMPORTANTE	Al reiniciar el switch se interrumpe la conectividad de los dispositivos con la red.

Desde la interface web del administrador de dispositivos, siga estos pasos.

1. Acceda al cuadro de diálogo Restart/Reset de la interface web del administrador de dispositivos.
2. Haga clic en Reset the Switch.

   Esta opción restablece el switch, borra los ajustes de configuración actuales, devuelve los ajustes predeterminados establecidos en fábrica y finalmente reinicia el switch.

   Si no conoce la dirección IP del switch, siga el procedimiento descrito en la sección Acceso al modo administrado directo en la página 209 para obtener acceso al modo administrado directo. A continuación, vuelva al paso 1, antes mencionado.

Recupere el firmware del switch y restaure los ajustes predeterminados establecidos en fábrica

Antes de que pueda recuperar el firmware del switch, debe asegurarse de lo siguiente:

- Deberá tener acceso físico al switch.
- Asegúrese de que se haya habilitado al menos un puerto del switch y de que no esté conectado a un dispositivo.

Si la imagen está alterada, puede recuperar el firmware del switch. Un síntoma de firmware alterado lo constituyen los repetidos intentos de reinicio del switch.

También será necesario realizar una recuperación de firmware del switch en caso de que se haya borrado la imagen debido a una actualización de firmware fallida o de que haya olvidado la contraseña del switch.

La recuperación del firmware del switch implica borrar todos los ajustes personalizados del switch y devolver al switch los ajustes predeterminados establecidos en fábrica. Para devolver al switch los ajustes predeterminados establecidos en fábrica, siga estos pasos.

1. Con el switch ya alimentado e iniciado, pulse y mantenga pulsado el botón Express Setup hasta que los indicadores de estado Setup y EIP Net se pongan rojos.

   Este proceso tarda aproximadamente 18…20 segundos en completarse.

2. Suelte el botón Express Setup.

3. Espere a que se reinicie el switch.

   El indicador Express Setup empieza a parpadear cuando el switch ha completado el reinicio. El switch ya tiene los ajustes predeterminados establecidos en fábrica.

4. Configure el switch, del modo descrito en Configure inicialmente el switch con Express Setup en la página 50.

5. Consulte Resuelva problemas de actualización de firmware en la página 212 y siga el procedimiento para actualizar el firmware.

Resuelva problemas de actualización de firmware

Si ha intentado actualizar el firmware del switch pero ha recibido un mensaje que indica que la actualización ha fallado, asegúrese de que aún tiene acceso al switch. Si aún tiene acceso al switch, siga estos pasos.

1. Asegúrese de haber descargado el archivo .tar correcto de http://www.rockwellautomation.com.

2. Si ha descargado el archivo .tar correcto, restaure la sesión del navegador de la interface web del administrador de dispositivos para asegurarse de que haya conectividad entre el switch y su computadora personal o unidad de red.
   - Si tiene conectividad con el switch y con la interface web del administrador de dispositivos, vuelva a intentar la actualización.
   - Si no tiene conectividad con el switch y con la interface web del administrador de dispositivos, consulte Recupere el firmware del switch y restaure los ajustes predeterminados establecidos en fábrica en la página 211.

Tipos de datos definidos por módulos

En la aplicación Logix Designer, los tags predefinidos para los tipos de datos de entrada y salida tienen una estructura que corresponde al switch seleccionado cuando se añadió al árbol de E/S. Los nombres de sus miembros se asignan de acuerdo con los nombres de los puertos.

Puede inhabilitar un puerto del switch, para lo cual debe establecer el bit correspondiente en el tag de salida. Los bits de salida se aplican cada vez que el switch recibe los datos de salida del controlador cuando el controlador está en modo de marcha. Cuando el controlador está en modo de programación, no se aplican los bits de salida.

El puerto está habilitado si el correspondiente bit de salida es 0. Si usted habilita o inhabilita un puerto utilizando la interface web del administrador de dispositivos o la CLI, el ajuste del puerto puede ser anulado por los bits de salida la próxima vez que se apliquen. Los bits de salida siempre tienen prioridad, independientemente de si se utilizó la interface web del administrador de dispositivos o la CLI para habilitar o inhabilitar el puerto.

Las tablas de este apéndice enumeran los tipos de datos definidos por módulos para los switches Stratix 5700. Las tablas incluyen información de entrada (indicada por una I) y de salida (indicada por una O).

Tipo de datos de entrada definidos por módulos (switches Gb de 6 puertos)

AB:STRATIX_5700_6PORT_GB_MANAGED:I:0			
Nombre de miembro	**Tipo**	**Estilo de visualización predeterminado**	**Valores válidos**
Fault	DINT	Binario	
AnyPortConnected	BOOL	Decimal	LinkStatus:0
PortFa1_1Connected	BOOL	Decimal	LinkStatus:1
PortFa1_2Connected	BOOL	Decimal	LinkStatus:2
PortFa1_3Connected	BOOL	Decimal	LinkStatus:3
PortFa1_4Connected	BOOL	Decimal	LinkStatus:4
PortGi1_1Connected	BOOL	Decimal	LinkStatus:5
PortGi1_2Connected	BOOL	Decimal	LinkStatus:6
AnyPortUnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:0
PortFa1_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:1
PortFa1_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:2
PortFa1_3UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:3
PortFa1_4UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:4
PortGi1_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:5
PortGi1_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:6
AnyPortThreshold	BOOL	Decimal	ThresholdExceeded:0
PortFa1_1Threshold	BOOL	Decimal	ThresholdExceeded:1
PortFa1_2Threshold	BOOL	Decimal	ThresholdExceeded:2
PortFa1_3Threshold	BOOL	Decimal	ThresholdExceeded:3
PortFa1_4Threshold	BOOL	Decimal	ThresholdExceeded:4
PortGi1_1Threshold	BOOL	Decimal	ThresholdExceeded:5
PortGi1_2Threshold	BOOL	Decimal	ThresholdExceeded:6
AllPortsUtilization	SINT	Decimal	
PortFa1_1Utilization	SINT	Decimal	
PortFa1_2Utilization	SINT	Decimal	
PortFa1_3Utilization	SINT	Decimal	
PortFa1_4Utilization	SINT	Decimal	
PortGi1_1Utilization	SINT	Decimal	
PortGi1_2Utilization	SINT	Decimal	
MajorAlarmRelay	BOOL	Decimal	AlarmRelay:0
MulticastGroupsActive	DINT	Binario	

Tipo de datos de salida definidos por módulos (switches Gb de 6 puertos)

AB:STRATIX_5700_6PORT_GB_MANAGED:O:0			
Nombre de miembro	**Tipo**	**Estilo de visualización predeterminado**	**Valores válidos**
AllPortsDisabled	BOOL	Decimal	DisablePort:0
PortFa1_1Disable	BOOL	Decimal	DisablePort:1
PortFa1_2Disable	BOOL	Decimal	DisablePort:2
PortFa1_3Disable	BOOL	Decimal	DisablePort:3
PortFa1_4Disable	BOOL	Decimal	DisablePort:4
PortGi1_1Disable	BOOL	Decimal	DisablePort:5
PortGi1_2Disable	BOOL	Decimal	DisablePort:6

Tipo de datos de entrada definidos por módulos (switches de 6 puertos)

AB:STRATIX_5700_6PORT_MANAGED:I:0			
Nombre de miembro	**Tipo**	**Estilo de visualización predeterminado**	**Valores válidos**
Fault	DINT	Binario	
AnyPortConnected	BOOL	Decimal	LinkStatus:0
PortFa1_1Connected	BOOL	Decimal	LinkStatus:1
PortFa1_2Connected	BOOL	Decimal	LinkStatus:2
PortFa1_3Connected	BOOL	Decimal	LinkStatus:3
PortFa1_4Connected	BOOL	Decimal	LinkStatus:4
PortFa1_5Connected	BOOL	Decimal	LinkStatus:5
PortFa1_6Connected	BOOL	Decimal	LinkStatus:6
AnyPortUnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:0
PortFa1_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:1
PortFa1_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:2
PortFa1_3UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:3
PortFa1_4UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:4
PortFa1_5UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:5
PortFa1_6UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:6
AnyPortThreshold	BOOL	Decimal	ThresholdExceeded:0
PortFa1_1Threshold	BOOL	Decimal	ThresholdExceeded:1
PortFa1_2Threshold	BOOL	Decimal	ThresholdExceeded:2
PortFa1_3Threshold	BOOL	Decimal	ThresholdExceeded:3
PortFa1_4Threshold	BOOL	Decimal	ThresholdExceeded:4
PortFa1_5Threshold	BOOL	Decimal	ThresholdExceeded:5
PortFa1_6Threshold	BOOL	Decimal	ThresholdExceeded:6
AllPortsUtilization	SINT	Decimal	
PortFa1_1Utilization	SINT	Decimal	
PortFa1_2Utilization	SINT	Decimal	
PortFa1_3Utilization	SINT	Decimal	
PortFa1_4Utilization	SINT	Decimal	
PortFa1_5Utilization	SINT	Decimal	

AB:STRATIX_5700_6PORT_MANAGED:I:0			
Nombre de miembro	**Tipo**	**Estilo de visualización predeterminado**	**Valores válidos**
PortFa1_6Utilization	SINT	Decimal	
MajorAlarmRelay	BOOL	Decimal	AlarmRelay:0
MulticastGroupsActive	DINT	Binario	

Tipo de datos de salida definidos por módulos (switches de 6 puertos)

AB:STRATIX_5700_6PORT_MANAGED:O:0			
Nombre de miembro	**Tipo**	**Estilo de visualización predeterminado**	**Valores válidos**
AllPortsDisabled	BOOL	Decimal	DisablePort:0
PortFa1_1Disable	BOOL	Decimal	DisablePort:1
PortFa1_2Disable	BOOL	Decimal	DisablePort:2
PortFa1_3Disable	BOOL	Decimal	DisablePort:3
PortFa1_4Disable	BOOL	Decimal	DisablePort:4
PortFa1_5Disable	BOOL	Decimal	DisablePort:5
PortFa1_6Disable	BOOL	Decimal	DisablePort:6

Tipo de datos de entrada definidos por módulos (switches Gb de 10 puertos)

AB:STRATIX_5700_10PORT_GB_MANAGED:I:0			
Nombre de miembro	**Tipo**	**Estilo de visualización predeterminado**	**Valores válidos**
Fault	DINT	Binario	
AnyPortConnected	BOOL	Decimal	LinkStatus:0
PortFa1_1Connected	BOOL	Decimal	LinkStatus:1
PortFa1_2Connected	BOOL	Decimal	LinkStatus:2
PortFa1_3Connected	BOOL	Decimal	LinkStatus:3
PortFa1_4Connected	BOOL	Decimal	LinkStatus:4
PortFa1_5Connected	BOOL	Decimal	LinkStatus:5
PortFa1_6Connected	BOOL	Decimal	LinkStatus:6
PortFa1_7Connected	BOOL	Decimal	LinkStatus:7
PortFa1_8Connected	BOOL	Decimal	LinkStatus:8
PortGi1_1Connected	BOOL	Decimal	LinkStatus:9
PortGi1_2Connected	BOOL	Decimal	LinkStatus:10
AnyPortUnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:0
PortFa1_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:1
PortFa1_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:2
PortFa1_3UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:3
PortFa1_4UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:4
PortFa1_5UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:5
PortFa1_6UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:6
PortFa1_7UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:7
PortFa1_8UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:8
PortGi1_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:9

AB:STRATIX_5700_10PORT_GB_MANAGED:I:0			
Nombre de miembro	**Tipo**	**Estilo de visualización predeterminado**	**Valores válidos**
PortGi1_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:10
AnyPortThreshold	BOOL	Decimal	ThresholdExceeded:0
PortFa1_1Threshold	BOOL	Decimal	ThresholdExceeded:1
PortFa1_2Threshold	BOOL	Decimal	ThresholdExceeded:2
PortFa1_3Threshold	BOOL	Decimal	ThresholdExceeded:3
PortFa1_4Threshold	BOOL	Decimal	ThresholdExceeded:4
PortFa1_5Threshold	BOOL	Decimal	ThresholdExceeded:5
PortFa1_6Threshold	BOOL	Decimal	ThresholdExceeded:6
PortFa1_7Threshold	BOOL	Decimal	ThresholdExceeded:7
PortFa1_8Threshold	BOOL	Decimal	ThresholdExceeded:8
PortGi1_1Threshold	BOOL	Decimal	ThresholdExceeded:9
PortGi1_2Threshold	BOOL	Decimal	ThresholdExceeded:10
AllPortsUtilization	SINT	Decimal	
PortFa1_1Utilization	SINT	Decimal	
PortFa1_2Utilization	SINT	Decimal	
PortFa1_3Utilization	SINT	Decimal	
PortFa1_4Utilization	SINT	Decimal	
PortFa1_5Utilization	SINT	Decimal	
PortFa1_6Utilization	SINT	Decimal	
PortFa1_7Utilization	SINT	Decimal	
PortFa1_8Utilization	SINT	Decimal	
PortGi1_1Utilization	SINT	Decimal	
PortGi1_2Utilization	SINT	Decimal	
MajorAlarmRelay	BOOL	Decimal	AlarmRelay:0
MulticastGroupsActive	DINT	Binario	

Tipo de datos de salida definidos por módulos (switches Gb de 10 puertos)

AB:STRATIX_5700_10PORT_MANAGED:0:0			
Nombre de miembro	**Tipo**	**Estilo de visualización predeterminado**	**Valores válidos**
AllPortsDisabled	BOOL	Decimal	DisablePort:0
PortFa1_1Disable	BOOL	Decimal	DisablePort:1
PortFa1_2Disable	BOOL	Decimal	DisablePort:2
PortFa1_3Disable	BOOL	Decimal	DisablePort:3
PortFa1_4Disable	BOOL	Decimal	DisablePort:4
PortFa1_5Disable	BOOL	Decimal	DisablePort:5
PortFa1_6Disable	BOOL	Decimal	DisablePort:6
PortFa1_7Disable	BOOL	Decimal	DisablePort:7
PortFa1_8Disable	BOOL	Decimal	DisablePort:8
PortGi1_1Disable	BOOL	Decimal	DisablePort:9
PortGi1_2Disable	BOOL	Decimal	DisablePort:10

Tipo de datos de entrada definidos por módulos (switches de 10 puertos)

AB:STRATIX_5700_10PORT_MANAGED:I:0			
Nombre de miembro	**Tipo**	**Estilo de visualización predeterminado**	**Valores válidos**
Fault	DINT	Binario	
AnyPortConnected	BOOL	Decimal	LinkStatus:0
PortFa1_1Connected	BOOL	Decimal	LinkStatus:1
PortFa1_2Connected	BOOL	Decimal	LinkStatus:2
PortFa1_3Connected	BOOL	Decimal	LinkStatus:3
PortFa1_4Connected	BOOL	Decimal	LinkStatus:4
PortFa1_5Connected	BOOL	Decimal	LinkStatus:5
PortFa1_6Connected	BOOL	Decimal	LinkStatus:6
PortFa1_7Connected	BOOL	Decimal	LinkStatus:7
PortFa1_8Connected	BOOL	Decimal	LinkStatus:8
PortFa1_9Connected	BOOL	Decimal	LinkStatus:9
PortFa1_10Connected	BOOL	Decimal	LinkStatus:10
AnyPortUnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:0
PortFa1_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:1
PortFa1_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:2
PortFa1_3UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:3
PortFa1_4UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:4
PortFa1_5UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:5
PortFa1_6UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:6
PortFa1_7UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:7
PortFa1_8UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:8
PortFa1_9UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:9
PortFa1_10UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:10
AnyPortThreshold	BOOL	Decimal	ThresholdExceeded:0
PortFa1_1Threshold	BOOL	Decimal	ThresholdExceeded:1
PortFa1_2Threshold	BOOL	Decimal	ThresholdExceeded:2

AB:STRATIX_5700_10PORT_MANAGED:I:0			
Nombre de miembro	**Tipo**	**Estilo de visualización predeterminado**	**Valores válidos**
PortFa1_3Threshold	BOOL	Decimal	ThresholdExceeded:3
PortFa1_4Threshold	BOOL	Decimal	ThresholdExceeded:4
PortFa1_5Threshold	BOOL	Decimal	ThresholdExceeded:5
PortFa1_6Threshold	BOOL	Decimal	ThresholdExceeded:6
PortFa1_7Threshold	BOOL	Decimal	ThresholdExceeded:7
PortFa1_8Threshold	BOOL	Decimal	ThresholdExceeded:8
PortFa1_9Threshold	BOOL	Decimal	ThresholdExceeded:9
PortFa1_10Threshold	BOOL	Decimal	ThresholdExceeded:10
AllPortsUtilization	SINT	Decimal	
PortFa1_1Utilization	SINT	Decimal	
PortFa1_2Utilization	SINT	Decimal	
PortFa1_3Utilization	SINT	Decimal	
PortFa1_4Utilization	SINT	Decimal	
PortFa1_5Utilization	SINT	Decimal	
PortFa1_6Utilization	SINT	Decimal	
PortFa1_7Utilization	SINT	Decimal	
PortFa1_8Utilization	SINT	Decimal	
PortFa1_9Utilization	SINT	Decimal	
PortFa1_10Utilization	SINT	Decimal	
MajorAlarmRelay	BOOL	Decimal	AlarmRelay:0
MulticastGroupsActive	DINT	Binario	

Tipo de datos de salida definidos por módulos (switches de 10 puertos)

AB:STRATIX_5700_10PORT_MANAGED:O:0			
Nombre de miembro	**Tipo**	**Estilo de visualización predeterminado**	**Valores válidos**
AllPortsDisabled	BOOL	Decimal	DisablePort:0
PortFa1_1Disable	BOOL	Decimal	DisablePort:1
PortFa1_2Disable	BOOL	Decimal	DisablePort:2
PortFa1_3Disable	BOOL	Decimal	DisablePort:3
PortFa1_4Disable	BOOL	Decimal	DisablePort:4
PortFa1_5Disable	BOOL	Decimal	DisablePort:5
PortFa1_6Disable	BOOL	Decimal	DisablePort:6
PortFa1_7Disable	BOOL	Decimal	DisablePort:7
PortFa1_8Disable	BOOL	Decimal	DisablePort:8
PortFa1_9Disable	BOOL	Decimal	DisablePort:9
PortFa1_10Disable	BOOL	Decimal	DisablePort:10

Tipo de datos de entrada definidos por módulos (switches Gb de 20 puertos)

AB:STRATIX_5700_20PORT_GB_MANAGED:I:0			
Nombre de miembro	**Tipo**	**Estilo de visualización predeterminado**	**Valores válidos**
Fault	DINT	Binario	
AnyPortConnected	BOOL	Decimal	LinkStatus:0
PortFa1_1Connected	BOOL	Decimal	LinkStatus:1
PortFa1_2Connected	BOOL	Decimal	LinkStatus:2
PortFa1_3Connected	BOOL	Decimal	LinkStatus:3
PortFa1_4Connected	BOOL	Decimal	LinkStatus:4
PortFa1_5Connected	BOOL	Decimal	LinkStatus:5
PortFa1_6Connected	BOOL	Decimal	LinkStatus:6
PortFa1_7Connected	BOOL	Decimal	LinkStatus:7
PortFa1_8Connected	BOOL	Decimal	LinkStatus:8
PortFa1_9Connected	BOOL	Decimal	LinkStatus:9
PortFa1_10Connected	BOOL	Decimal	LinkStatus:10
PortFa1_11Connected	BOOL	Decimal	LinkStatus:11
PortFa1_12Connected	BOOL	Decimal	LinkStatus:12
PortFa1_13Connected	BOOL	Decimal	LinkStatus:13
PortFa1_14Connected	BOOL	Decimal	LinkStatus:14
PortFa1_15Connected	BOOL	Decimal	LinkStatus:15
PortFa1_16Connected	BOOL	Decimal	LinkStatus:16
PortFa1_17Connected	BOOL	Decimal	LinkStatus:17
PortFa1_18Connected	BOOL	Decimal	LinkStatus:18
PortGi1_1Connected	BOOL	Decimal	LinkStatus:19
PortGi1_2Connected	BOOL	Decimal	LinkStatus:20
AnyPortUnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:0
PortFa1_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:1
PortFa1_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:2
PortFa1_3UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:3
PortFa1_4UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:4
PortFa1_5UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:5
PortFa1_6UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:6
PortFa1_7UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:7
PortFa1_8UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:8
PortFa1_9UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:9
PortFa1_10UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:10
PortFa1_11UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:11
PortFa1_12UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:12
PortFa1_13UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:13
PortFa1_14UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:14
PortFa1_15UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:15
PortFa1_16UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:16
PortFa1_17UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:17
PortFa1_18UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:18
PortGi1_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:19

AB:STRATIX_5700_20PORT_GB_MANAGED:I:0			
Nombre de miembro	**Tipo**	**Estilo de visualización predeterminado**	**Valores válidos**
PortGi1_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:20
AnyPortThreshold	BOOL	Decimal	ThresholdExceeded:0
PortFa1_1Threshold	BOOL	Decimal	ThresholdExceeded:1
PortFa1_2Threshold	BOOL	Decimal	ThresholdExceeded:2
PortFa1_3Threshold	BOOL	Decimal	ThresholdExceeded:3
PortFa1_4Threshold	BOOL	Decimal	ThresholdExceeded:4
PortFa1_5Threshold	BOOL	Decimal	ThresholdExceeded:5
PortFa1_6Threshold	BOOL	Decimal	ThresholdExceeded:6
PortFa1_7Threshold	BOOL	Decimal	ThresholdExceeded:7
PortFa1_8Threshold	BOOL	Decimal	ThresholdExceeded:8
PortFa1_9Threshold	BOOL	Decimal	ThresholdExceeded:9
PortFa1_10Threshold	BOOL	Decimal	ThresholdExceeded:10
PortFa1_11Threshold	BOOL	Decimal	ThresholdExceeded:11
PortFa1_12Threshold	BOOL	Decimal	ThresholdExceeded:12
PortFa1_13Threshold	BOOL	Decimal	ThresholdExceeded:13
PortFa1_14Threshold	BOOL	Decimal	ThresholdExceeded:14
PortFa1_15Threshold	BOOL	Decimal	ThresholdExceeded:15
PortFa1_16Threshold	BOOL	Decimal	ThresholdExceeded:16
PortFa1_17Threshold	BOOL	Decimal	ThresholdExceeded:17
PortFa1_18Threshold	BOOL	Decimal	ThresholdExceeded:18
PortGi1_1Threshold	BOOL	Decimal	ThresholdExceeded:19
PortGi1_2Threshold	BOOL	Decimal	ThresholdExceeded:20
AllPortsUtilization	SINT	Decimal	
PortFa1_1Utilization	SINT	Decimal	
PortFa1_2Utilization	SINT	Decimal	
PortFa1_3Utilization	SINT	Decimal	
PortFa1_4Utilization	SINT	Decimal	
PortFa1_5Utilization	SINT	Decimal	
PortFa1_6Utilization	SINT	Decimal	
PortFa1_7Utilization	SINT	Decimal	
PortFa1_8Utilization	SINT	Decimal	
PortFa1_9Utilization	SINT	Decimal	
PortFa1_10Utilization	SINT	Decimal	
PortFa1_11Utilization	SINT	Decimal	
PortFa1_12Utilization	SINT	Decimal	
PortFa1_13Utilization	SINT	Decimal	
PortFa1_14Utilization	SINT	Decimal	
PortFa1_15Utilization	SINT	Decimal	
PortFa1_16Utilization	SINT	Decimal	
PortFa1_17Utilization	SINT	Decimal	
PortFa1_18Utilization	SINT	Decimal	
PortGi1_1Utilization	SINT	Decimal	

AB:STRATIX_5700_20PORT_GB_MANAGED:I:0			
Nombre de miembro	**Tipo**	**Estilo de visualización predeterminado**	**Valores válidos**
PortGi1_2Utilization	SINT	Decimal	
MajorAlarmRelay	BOOL	Decimal	AlarmRelay:0
MulticastGroupsActive	DINT	Binario	

Tipo de datos de entrada definidos por módulos (switches Gb de 18 puertos)

AB:STRATIX_5700_18PORT_GB_MANAGED:I:0			
Nombre de miembro	**Tipo**	**Estilo de visualización predeterminado**	**Valores válidos**
Fault	DINT	Binario	
AnyPortConnected	BOOL	Decimal	LinkStatus:0
PortFa1_1Connected	BOOL	Decimal	LinkStatus:1
PortFa1_2Connected	BOOL	Decimal	LinkStatus:2
PortFa1_3Connected	BOOL	Decimal	LinkStatus:3
PortFa1_4Connected	BOOL	Decimal	LinkStatus:4
PortFa1_5Connected	BOOL	Decimal	LinkStatus:5
PortFa1_6Connected	BOOL	Decimal	LinkStatus:6
PortFa1_7Connected	BOOL	Decimal	LinkStatus:7
PortFa1_8Connected	BOOL	Decimal	LinkStatus:8
PortFa1_9Connected	BOOL	Decimal	LinkStatus:9
PortFa1_10Connected	BOOL	Decimal	LinkStatus:10
PortFa1_11Connected	BOOL	Decimal	LinkStatus:11
PortFa1_12Connected	BOOL	Decimal	LinkStatus:12
PortFa1_13Connected	BOOL	Decimal	LinkStatus:13
PortFa1_14Connected	BOOL	Decimal	LinkStatus:14
PortFa1_15Connected	BOOL	Decimal	LinkStatus:15
PortFa1_16Connected	BOOL	Decimal	LinkStatus:16
PortGi1_1Connected	BOOL	Decimal	LinkStatus:19
PortGi1_2Connected	BOOL	Decimal	LinkStatus:20
AnyPortUnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:0
PortFa1_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:1
PortFa1_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:2
PortFa1_3UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:3
PortFa1_4UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:4
PortFa1_5UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:5
PortFa1_6UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:6
PortFa1_7UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:7
PortFa1_8UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:8
PortFa1_9UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:9
PortFa1_10UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:10
PortFa1_11UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:11
PortFa1_12UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:12
PortFa1_13UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:13

AB:STRATIX_5700_18PORT_GB_MANAGED:I:0			
Nombre de miembro	**Tipo**	**Estilo de visualización predeterminado**	**Valores válidos**
PortFa1_14UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:14
PortFa1_15UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:15
PortFa1_16UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:16
PortGi1_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:19
PortGi1_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:20
AnyPortThreshold	BOOL	Decimal	ThresholdExceeded:0
PortFa1_1Threshold	BOOL	Decimal	ThresholdExceeded:1
PortFa1_2Threshold	BOOL	Decimal	ThresholdExceeded:2
PortFa1_3Threshold	BOOL	Decimal	ThresholdExceeded:3
PortFa1_4Threshold	BOOL	Decimal	ThresholdExceeded:4
PortFa1_5Threshold	BOOL	Decimal	ThresholdExceeded:5
PortFa1_6Threshold	BOOL	Decimal	ThresholdExceeded:6
PortFa1_7Threshold	BOOL	Decimal	ThresholdExceeded:7
PortFa1_8Threshold	BOOL	Decimal	ThresholdExceeded:8
PortFa1_9Threshold	BOOL	Decimal	ThresholdExceeded:9
PortFa1_10Threshold	BOOL	Decimal	ThresholdExceeded:10
PortFa1_11Threshold	BOOL	Decimal	ThresholdExceeded:11
PortFa1_12Threshold	BOOL	Decimal	ThresholdExceeded:12
PortFa1_13Threshold	BOOL	Decimal	ThresholdExceeded:13
PortFa1_14Threshold	BOOL	Decimal	ThresholdExceeded:14
PortFa1_15Threshold	BOOL	Decimal	ThresholdExceeded:15
PortFa1_16Threshold	BOOL	Decimal	ThresholdExceeded:16
PortGi1_1Threshold	BOOL	Decimal	ThresholdExceeded:19
PortGi1_2Threshold	BOOL	Decimal	ThresholdExceeded:20
AllPortsUtilization	SINT	Decimal	
PortFa1_1Utilization	SINT	Decimal	
PortFa1_2Utilization	SINT	Decimal	
PortFa1_3Utilization	SINT	Decimal	
PortFa1_4Utilization	SINT	Decimal	
PortFa1_5Utilization	SINT	Decimal	
PortFa1_6Utilization	SINT	Decimal	
PortFa1_7Utilization	SINT	Decimal	
PortFa1_8Utilization	SINT	Decimal	
PortFa1_9Utilization	SINT	Decimal	
PortFa1_10Utilization	SINT	Decimal	
PortFa1_11Utilization	SINT	Decimal	
PortFa1_12Utilization	SINT	Decimal	
PortFa1_13Utilization	SINT	Decimal	
PortFa1_14Utilization	SINT	Decimal	
PortFa1_15Utilization	SINT	Decimal	
PortFa1_16Utilization	SINT	Decimal	
PortGi1_1Utilization	SINT	Decimal	

AB:STRATIX_5700_18PORT_GB_MANAGED:I:0			
Nombre de miembro	**Tipo**	**Estilo de visualización predeterminado**	**Valores válidos**
PortGi1_2Utilization	SINT	Decimal	
MajorAlarmRelay	BOOL	Decimal	AlarmRelay:0
MulticastGroupsActive	DINT	Binario	

Tipo de datos de salida definidos por módulos (switches Gb de 18 puertos)

AB:STRATIX_5700_18PORT_GB_MANAGED:O:0			
Nombre de miembro	**Tipo**	**Estilo de visualización predeterminado**	**Valores válidos**
AllPortsDisabled	BOOL	Decimal	DisablePort:0
PortFa1_1Disable	BOOL	Decimal	DisablePort:1
PortFa1_2Disable	BOOL	Decimal	DisablePort:2
PortFa1_3Disable	BOOL	Decimal	DisablePort:3
PortFa1_4Disable	BOOL	Decimal	DisablePort:4
PortFa1_5Disable	BOOL	Decimal	DisablePort:5
PortFa1_6Disable	BOOL	Decimal	DisablePort:6
PortFa1_7Disable	BOOL	Decimal	DisablePort:7
PortFa1_8Disable	BOOL	Decimal	DisablePort:8
PortFa1_9Disable	BOOL	Decimal	DisablePort:9
PortFa1_10Disable	BOOL	Decimal	DisablePort:10
PortFa1_11Disable	BOOL	Decimal	DisablePort:11
PortFa1_12Disable	BOOL	Decimal	DisablePort:12
PortFa1_13Disable	BOOL	Decimal	DisablePort:13
PortFa1_14Disable	BOOL	Decimal	DisablePort:14
PortFa1_15Disable	BOOL	Decimal	DisablePort:15
PortFa1_16Disable	BOOL	Decimal	DisablePort:16
PortGi1_1Disable	BOOL	Decimal	DisablePort:19
PortGi1_2Disable	BOOL	Decimal	DisablePort:20

Tipo de datos de entrada definidos por módulos (switches Gb de 20 puertos)

AB:STRATIX_5700_20PORT_GB_MANAGED:I:0			
Nombre de miembro	**Tipo**	**Estilo de visualización predeterminado**	**Valores válidos**
Fault	DINT	Binario	
AnyPortConnected	BOOL	Decimal	LinkStatus:0
PortFa1_1Connected	BOOL	Decimal	LinkStatus:1
PortFa1_2Connected	BOOL	Decimal	LinkStatus:2
PortFa1_3Connected	BOOL	Decimal	LinkStatus:3
PortFa1_4Connected	BOOL	Decimal	LinkStatus:4
PortFa1_5Connected	BOOL	Decimal	LinkStatus:5
PortFa1_6Connected	BOOL	Decimal	LinkStatus:6
PortFa1_7Connected	BOOL	Decimal	LinkStatus:7
PortFa1_8Connected	BOOL	Decimal	LinkStatus:8
PortFa1_9Connected	BOOL	Decimal	LinkStatus:9
PortFa1_10Connected	BOOL	Decimal	LinkStatus:10
PortFa1_11Connected	BOOL	Decimal	LinkStatus:11
PortFa1_12Connected	BOOL	Decimal	LinkStatus:12
PortFa1_13Connected	BOOL	Decimal	LinkStatus:13
PortFa1_14Connected	BOOL	Decimal	LinkStatus:14
PortFa1_15Connected	BOOL	Decimal	LinkStatus:15
PortFa1_16Connected	BOOL	Decimal	LinkStatus:16
PortFa1_17Connected	BOOL	Decimal	LinkStatus:17
PortFa1_18Connected	BOOL	Decimal	LinkStatus:18
PortGi1_1Connected	BOOL	Decimal	LinkStatus:19
PortGi1_2Connected	BOOL	Decimal	LinkStatus:20
AnyPortUnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:0
PortFa1_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:1
PortFa1_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:2
PortFa1_3UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:3
PortFa1_4UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:4
PortFa1_5UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:5
PortFa1_6UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:6
PortFa1_7UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:7
PortFa1_8UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:8
PortFa1_9UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:9
PortFa1_10UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:10
PortFa1_11UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:11
PortFa1_12UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:12
PortFa1_13UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:13
PortFa1_14UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:14
PortFa1_15UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:15
PortFa1_16UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:16
PortFa1_17UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:17
PortFa1_18UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:18
PortGi1_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:19

AB:STRATIX_5700_20PORT_GB_MANAGED:I:0			
Nombre de miembro	**Tipo**	**Estilo de visualización predeterminado**	**Valores válidos**
PortGi1_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:20
AnyPortThreshold	BOOL	Decimal	ThresholdExceeded:0
PortFa1_1Threshold	BOOL	Decimal	ThresholdExceeded:1
PortFa1_2Threshold	BOOL	Decimal	ThresholdExceeded:2
PortFa1_3Threshold	BOOL	Decimal	ThresholdExceeded:3
PortFa1_4Threshold	BOOL	Decimal	ThresholdExceeded:4
PortFa1_5Threshold	BOOL	Decimal	ThresholdExceeded:5
PortFa1_6Threshold	BOOL	Decimal	ThresholdExceeded:6
PortFa1_7Threshold	BOOL	Decimal	ThresholdExceeded:7
PortFa1_8Threshold	BOOL	Decimal	ThresholdExceeded:8
PortFa1_9Threshold	BOOL	Decimal	ThresholdExceeded:9
PortFa1_10Threshold	BOOL	Decimal	ThresholdExceeded:10
PortFa1_11Threshold	BOOL	Decimal	ThresholdExceeded:11
PortFa1_12Threshold	BOOL	Decimal	ThresholdExceeded:12
PortFa1_13Threshold	BOOL	Decimal	ThresholdExceeded:13
PortFa1_14Threshold	BOOL	Decimal	ThresholdExceeded:14
PortFa1_15Threshold	BOOL	Decimal	ThresholdExceeded:15
PortFa1_16Threshold	BOOL	Decimal	ThresholdExceeded:16
PortFa1_17Threshold	BOOL	Decimal	ThresholdExceeded:17
PortFa1_18Threshold	BOOL	Decimal	ThresholdExceeded:18
PortGi1_1Threshold	BOOL	Decimal	ThresholdExceeded:19
PortGi1_2Threshold	BOOL	Decimal	ThresholdExceeded:20
AllPortsUtilization	SINT	Decimal	
PortFa1_1Utilization	SINT	Decimal	
PortFa1_2Utilization	SINT	Decimal	
PortFa1_3Utilization	SINT	Decimal	
PortFa1_4Utilization	SINT	Decimal	
PortFa1_5Utilization	SINT	Decimal	
PortFa1_6Utilization	SINT	Decimal	
PortFa1_7Utilization	SINT	Decimal	
PortFa1_8Utilization	SINT	Decimal	
PortFa1_9Utilization	SINT	Decimal	
PortFa1_10Utilization	SINT	Decimal	
PortFa1_11Utilization	SINT	Decimal	
PortFa1_12Utilization	SINT	Decimal	
PortFa1_13Utilization	SINT	Decimal	
PortFa1_14Utilization	SINT	Decimal	
PortFa1_15Utilization	SINT	Decimal	
PortFa1_16Utilization	SINT	Decimal	
PortFa1_17Utilization	SINT	Decimal	
PortFa1_18Utilization	SINT	Decimal	
PortGi1_1Utilization	SINT	Decimal	

AB:STRATIX_5700_20PORT_GB_MANAGED:I:0			
Nombre de miembro	**Tipo**	**Estilo de visualización predeterminado**	**Valores válidos**
PortGi1_2Utilization	SINT	Decimal	
MajorAlarmRelay	BOOL	Decimal	AlarmRelay:0
MulticastGroupsActive	DINT	Binario	

Tipo de datos de salida definidos por módulos (switches Gb de 20 puertos)

AB:STRATIX_5700_20PORT_GB_MANAGED:O:0			
Nombre de miembro	**Tipo**	**Estilo de visualización predeterminado**	**Valores válidos**
AllPortsDisabled	BOOL	Decimal	DisablePort:0
PortFa1_1Disable	BOOL	Decimal	DisablePort:1
PortFa1_2Disable	BOOL	Decimal	DisablePort:2
PortFa1_3Disable	BOOL	Decimal	DisablePort:3
PortFa1_4Disable	BOOL	Decimal	DisablePort:4
PortFa1_5Disable	BOOL	Decimal	DisablePort:5
PortFa1_6Disable	BOOL	Decimal	DisablePort:6
PortFa1_7Disable	BOOL	Decimal	DisablePort:7
PortFa1_8Disable	BOOL	Decimal	DisablePort:8
PortFa1_9Disable	BOOL	Decimal	DisablePort:9
PortFa1_10Disable	BOOL	Decimal	DisablePort:10
PortFa1_11Disable	BOOL	Decimal	DisablePort:11
PortFa1_12Disable	BOOL	Decimal	DisablePort:12
PortFa1_13Disable	BOOL	Decimal	DisablePort:13
PortFa1_14Disable	BOOL	Decimal	DisablePort:14
PortFa1_15Disable	BOOL	Decimal	DisablePort:15
PortFa1_16Disable	BOOL	Decimal	DisablePort:16
PortFa1_17Disable	BOOL	Decimal	DisablePort:17
PortFa1_18Disable	BOOL	Decimal	DisablePort:18
PortGi1_1Disable	BOOL	Decimal	DisablePort:19
PortGi1_2Disable	BOOL	Decimal	DisablePort:20

Tipo de datos de entrada definidos por módulos (switches de 20 puertos)

AB:STRATIX_5700_20PORT_MANAGED:I:0			
Nombre de miembro	**Tipo**	**Estilo de visualización predeterminado**	**Valores válidos**
Fault	DINT	Binario	
AnyPortConnected	BOOL	Decimal	LinkStatus:0
PortFa1_1Connected	BOOL	Decimal	LinkStatus:1
PortFa1_2Connected	BOOL	Decimal	LinkStatus:2
PortFa1_3Connected	BOOL	Decimal	LinkStatus:3
PortFa1_4Connected	BOOL	Decimal	LinkStatus:4
PortFa1_5Connected	BOOL	Decimal	LinkStatus:5
PortFa1_6Connected	BOOL	Decimal	LinkStatus:6
PortFa1_7Connected	BOOL	Decimal	LinkStatus:7
PortFa1_8Connected	BOOL	Decimal	LinkStatus:8
PortFa1_9Connected	BOOL	Decimal	LinkStatus:9
PortFa1_10Connected	BOOL	Decimal	LinkStatus:10
PortFa1_11Connected	BOOL	Decimal	LinkStatus:11
PortFa1_12Connected	BOOL	Decimal	LinkStatus:12
PortFa1_13Connected	BOOL	Decimal	LinkStatus:13
PortFa1_14Connected	BOOL	Decimal	LinkStatus:14
PortFa1_15Connected	BOOL	Decimal	LinkStatus:15
PortFa1_16Connected	BOOL	Decimal	LinkStatus:16
PortFa1_17Connected	BOOL	Decimal	LinkStatus:17
PortFa1_18Connected	BOOL	Decimal	LinkStatus:18
PortFa1_19Connected	BOOL	Decimal	LinkStatus:19
PortFa1_20Connected	BOOL	Decimal	LinkStatus:20
AnyPortUnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:0
PortFa1_1UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:1
PortFa1_2UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:2
PortFa1_3UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:3
PortFa1_4UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:4
PortFa1_5UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:5
PortFa1_6UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:6
PortFa1_7UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:7
PortFa1_8UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:8
PortFa1_9UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:9
PortFa1_10UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:10
PortFa1_11UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:11
PortFa1_12UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:12
PortFa1_13UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:13
PortFa1_14UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:14
PortFa1_15UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:15
PortFa1_16UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:16
PortFa1_17UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:17
PortFa1_18UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:18
PortFa1_19UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:19

AB:STRATIX_5700_20PORT_MANAGED:I:0			
Nombre de miembro	**Tipo**	**Estilo de visualización predeterminado**	**Valores válidos**
PortFa1_20UnauthorizedDevice	BOOL	Decimal	UnauthorizedDevice:20
AnyPortThreshold	BOOL	Decimal	ThresholdExceeded:0
PortFa1_1Threshold	BOOL	Decimal	ThresholdExceeded:1
PortFa1_2Threshold	BOOL	Decimal	ThresholdExceeded:2
PortFa1_3Threshold	BOOL	Decimal	ThresholdExceeded:3
PortFa1_4Threshold	BOOL	Decimal	ThresholdExceeded:4
PortFa1_5Threshold	BOOL	Decimal	ThresholdExceeded:5
PortFa1_6Threshold	BOOL	Decimal	ThresholdExceeded:6
PortFa1_7Threshold	BOOL	Decimal	ThresholdExceeded:7
PortFa1_8Threshold	BOOL	Decimal	ThresholdExceeded:8
PortFa1_9Threshold	BOOL	Decimal	ThresholdExceeded:9
PortFa1_10Threshold	BOOL	Decimal	ThresholdExceeded:10
PortFa1_11Threshold	BOOL	Decimal	ThresholdExceeded:11
PortFa1_12Threshold	BOOL	Decimal	ThresholdExceeded:12
PortFa1_13Threshold	BOOL	Decimal	ThresholdExceeded:13
PortFa1_14Threshold	BOOL	Decimal	ThresholdExceeded:14
PortFa1_15Threshold	BOOL	Decimal	ThresholdExceeded:15
PortFa1_16Threshold	BOOL	Decimal	ThresholdExceeded:16
PortFa1_17Threshold	BOOL	Decimal	ThresholdExceeded:17
PortFa1_18Threshold	BOOL	Decimal	ThresholdExceeded:18
PortFa1_19Threshold	BOOL	Decimal	ThresholdExceeded:19
PortFa1_20Threshold	BOOL	Decimal	ThresholdExceeded:20
AllPortsUtilization	SINT	Decimal	
PortFa1_1Utilization	SINT	Decimal	
PortFa1_2Utilization	SINT	Decimal	
PortFa1_3Utilization	SINT	Decimal	
PortFa1_4Utilization	SINT	Decimal	
PortFa1_5Utilization	SINT	Decimal	
PortFa1_6Utilization	SINT	Decimal	
PortFa1_7Utilization	SINT	Decimal	
PortFa1_8Utilization	SINT	Decimal	
PortFa1_9Utilization	SINT	Decimal	
PortFa1_10Utilization	SINT	Decimal	
PortFa1_11Utilization	SINT	Decimal	
PortFa1_12Utilization	SINT	Decimal	
PortFa1_13Utilization	SINT	Decimal	
PortFa1_14Utilization	SINT	Decimal	
PortFa1_15Utilization	SINT	Decimal	
PortFa1_16Utilization	SINT	Decimal	
PortFa1_17Utilization	SINT	Decimal	
PortFa1_18Utilization	SINT	Decimal	
PortFa1_19Utilization	SINT	Decimal	

AB:STRATIX_5700_20PORT_MANAGED:I:0			
Nombre de miembro	**Tipo**	**Estilo de visualización predeterminado**	**Valores válidos**
PortFa1_20Utilization	SINT	Decimal	
MajorAlarmRelay	BOOL	Decimal	AlarmRelay:0
MulticastGroupsActive	DINT	Binario	

Tipo de datos de salida definidos por módulos (switches de 20 puertos)

AB:STRATIX_5700_20PORT_MANAGED:O:0			
Nombre de miembro	**Tipo**	**Estilo de visualización predeterminado**	**Valores válidos**
AllPortsDisabled	BOOL	Decimal	DisablePort:0
PortFa1_1Disable	BOOL	Decimal	DisablePort:1
PortFa1_2Disable	BOOL	Decimal	DisablePort:2
PortFa1_3Disable	BOOL	Decimal	DisablePort:3
PortFa1_4Disable	BOOL	Decimal	DisablePort:4
PortFa1_5Disable	BOOL	Decimal	DisablePort:5
PortFa1_6Disable	BOOL	Decimal	DisablePort:6
PortFa1_7Disable	BOOL	Decimal	DisablePort:7
PortFa1_8Disable	BOOL	Decimal	DisablePort:8
PortFa1_9Disable	BOOL	Decimal	DisablePort:9
PortFa1_10Disable	BOOL	Decimal	DisablePort:10
PortFa1_11Disable	BOOL	Decimal	DisablePort:11
PortFa1_12Disable	BOOL	Decimal	DisablePort:12
PortFa1_13Disable	BOOL	Decimal	DisablePort:13
PortFa1_14Disable	BOOL	Decimal	DisablePort:14
PortFa1_15Disable	BOOL	Decimal	DisablePort:15
PortFa1_16Disable	BOOL	Decimal	DisablePort:16
PortFa1_17Disable	BOOL	Decimal	DisablePort:17
PortFa1_18Disable	BOOL	Decimal	DisablePort:18
PortFa1_19Disable	BOOL	Decimal	DisablePort:19
PortFa1_20Disable	BOOL	Decimal	DisablePort:20

Asignaciones de puertos para datos CIP

Esta tabla identifica los números de ocurrencia del objeto de vínculo Ethernet asociado con cada puerto del switch. La ocurrencia 0 no se aplica a todos los puertos como se aplica a los mapas de bits.

Los números de bit identifican cada puerto cuando están contenidos en una estructura de todos los puertos, como en el conjunto de salida. El bit 0 hace referencia a cualquiera o a todos los puertos.

Ocurrencia/bit	Switch de 6 puertos	Switch Gb de 6 puertos	Switch de 10 puertos	Switch Gb de 10 puertos	Switch Gb de 18 puertos	Switch de 20 puertos	Switch Gb de 20 puertos
Bit 0	Cualquier puerto/ todos los puertos	Cualquier puerto/ todos los puertos	Cualquier puerto/ todos los puertos	Cualquier puerto/ todos los puertos	Cualquier puerto/ todos los puertos	Cualquier puerto/ todos los puertos	Cualquier puerto/ todos los puertos
Ocurrencia/bit 1	Fa1/1	Fa/1	Fa1/1	Fa1/1	Fa1/1	Fa1/1	Fa1/1
Ocurrencia/bit 2	Fa1/2	Fa1/2	Fa1/2	Fa1/2	Fa1/2	Fa1/2	Fa1/2
Ocurrencia/bit 3	Fa1/3	Fa1/3	Fa1/3	Fa1/3	Fa1/3	Fa1/3	Fa1/3
Ocurrencia/bit 4	Fa1/4	Fa1/4	Fa1/4	Fa1/4	Fa1/4	Fa1/4	Fa1/4
Ocurrencia/bit 5	Fa1/5	Gi1/1	Fa1/5	Fa1/5	Fa1/5	Fa1/5	Fa1/5
Ocurrencia/bit 6	Fa1/6	Gi1/2	Fa1/6	Fa1/6	Fa1/6	Fa1/6	Fa1/6
Ocurrencia/bit 7			Fa1/7	Fa1/7	Fa1/7	Fa1/7	Fa1/7
Ocurrencia/bit 8			Fa1/8	Fa1/8	Fa1/8	Fa1/8	Fa1/8
Ocurrencia/bit 9			Fa1/9	Gi1/1	Fa1/9	Fa1/9	Fa1/9
Ocurrencia/bit 10			Fa1/10	Gi1/2	Fa1/10	Fa1/10	Fa1/10
Ocurrencia/bit 11					Fa1/11	Fa1/11	Fa1/11
Ocurrencia/bit 12					Fa1/12	Fa1/12	Fa1/12
Ocurrencia/bit 13					Fa1/13	Fa1/13	Fa1/13
Ocurrencia/bit 14					Fa1/14	Fa1/14	Fa1/14
Ocurrencia/bit 15					Fa1/15	Fa1/15	Fa1/15
Ocurrencia/bit 16					Fa1/16	Fa1/16	Fa1/16
Ocurrencia/bit 17						Fa1/17	Fa1/17
Ocurrencia/bit 18						Fa1/18	Fa1/18
Ocurrencia/bit 19					Gi1/1	Fa1/19	Gi1/1
Ocurrencia/bit 20					Gi1/2	Fa1/20	Gi1/2
Ocurrencia/bit 27	SVI1	SVI1	SVI1	SVI1	SVI1	SVI1	SVI1

Notas:

Cables y conectores

Puertos 10/100 y 10/100/1000

Los puertos Ethernet 10/100 y 10/100/1000 en los switches utilizan conectores RJ45 estándar y configuraciones de pines Ethernet con cruces internos.

SUGERENCIA La característica Auto-MDIX está habilitada de forma predeterminada.

Figura 10 - Configuraciones de pines del conector 10/100

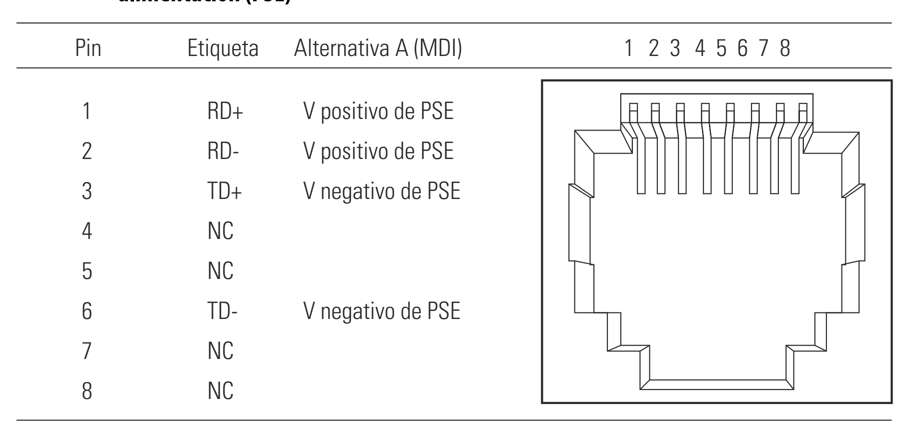
Pin	Etiqueta
1	RD+
2	RD-
3	TD+
4	NC
5	NC
6	TD-
7	NC
8	NC

Figura 11 - Configuraciones de pines del conector 10/100/1000

Pin	Etiqueta
1	TP0+
2	TP0-
3	TP1+
4	TP2+
5	TP2-
6	TP1-
7	TP3+
8	TP3-

Los puertos PoE integran señales de alimentación y de datos en los mismos cables. Los puertos utilizan conectores RJ45 estándar y configuraciones de pines Ethernet con cruces internos.

Figura 12 - Configuraciones de pines del conector PoE 10/100 y voltaje del equipo de fuente de alimentación (PSE)



Pin	Etiqueta	Alternativa A (MDI)
1	RD+	V positivo de PSE
2	RD-	V positivo de PSE
3	TD+	V negativo de PSE
4	NC	
5	NC	
6	TD-	V negativo de PSE
7	NC	
8	NC	

Conecte a dispositivos compatibles con 10BASE-T- y 100BASE-TX

La característica Auto-MDIX está habilitada de forma predeterminada. Siga las pautas de cableado siguientes cuando se ha inhabilitado la característica Auto-MDIX.

Al conectar los puertos a dispositivos compatibles 10BASE-T y 100BASE-TX, como servidores, estaciones de trabajo y encaminadores, puede utilizar un cable de tipo directo de dos o cuatro pares trenzados para 10BASE-T y 100BASE-TX.

Para identificar un cable cruzado, compare los dos extremos modulares del cable. Sujete los extremos del cable uno al lado del otro, con la lengüeta en la parte posterior. El cable conectado al pin en el extremo izquierdo del conector de la izquierda debe ser de un color diferente al del cable conectado al pin en el extremo izquierdo del conector de la derecha.

Las siguientes figuras muestran estos esquemas:

- Cable de tipo directo con dos pares trenzados
- Cable de tipo directo con cuatro pares trenzados

Figura 13 - Esquema de cable de tipo directo con dos pares trenzados

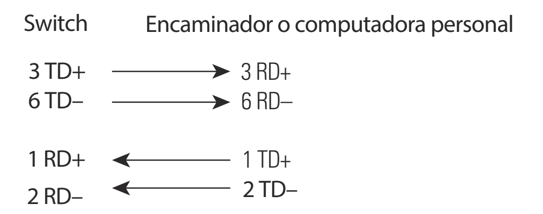
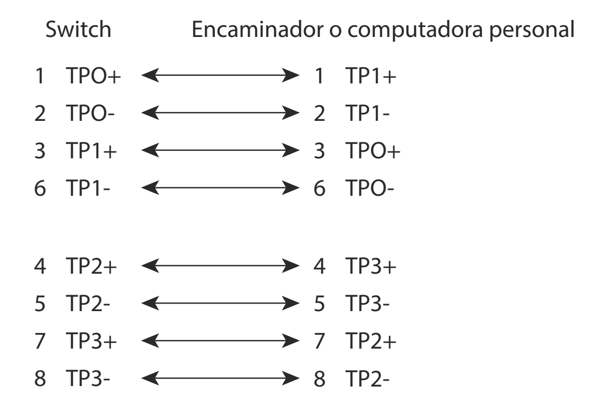


Figura 14 - Esquema de cable de tipo directo con cuatro pares trenzados



Cuando se conectan los puertos a dispositivos compatibles con 10BASE-T y 100BASE-TX, como switches o repetidores, puede utilizar un cable cruzado de dos o de cuatro pares trenzados.

Las siguientes figuras muestran estos esquemas:

- Esquema de cable cruzado de dos pares trenzados
- Esquema de cable cruzado de cuatro pares trenzados

Utilice un cable de tipo directo para conectar dos puertos cuando solo se ha designado un puerto con una X. Utilice un cable cruzado para conectar dos puertos cuando ambos puertos están designados con una X o cuando ambos puertos no tienen una X.

Puede utilizar cables de categoría 3, 4 o 5 para la conexión a dispositivos compatibles con 10BASE-T. Debe utilizar cables de categoría 5 para la conexión a dispositivos compatibles con 100BASE-TX.

IMPORTANTE	Utilice cable de cuatro pares trenzados de categoría 5 para la conexión a dispositivos compatibles con 1000BASE-T o puertos PoE.

Figura 15 - Esquema de cable cruzado de dos pares trenzados

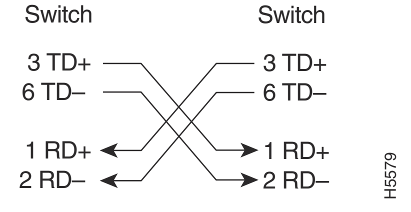
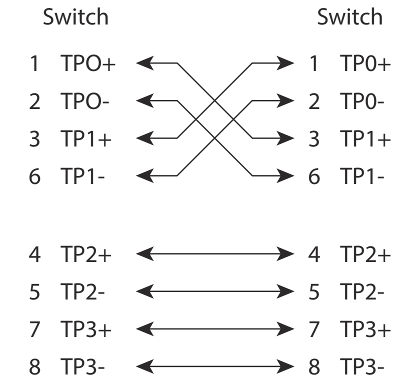


Figura 16 - Esquema de cable cruzado de cuatro pares trenzados



Puertos de doble función (puertos combinados)

El puerto Ethernet en un puerto de doble función utiliza conectores RJ45 estándar. La figura siguiente muestra las configuraciones de pines.

Figura 17 - Conector RJ45 de puerto Ethernet

Pin	Etiqueta
1	TP0+
2	TP0-
3	TP1+
4	TP2+
5	TP2-
6	TP1-
7	TP3+
8	TP3-

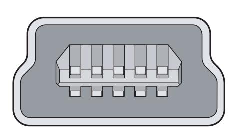
1 2 3 4 5 6 7 8

La ranura del módulo SFP en un puerto de doble función emplea módulos SFP para puertos de fibra óptica.

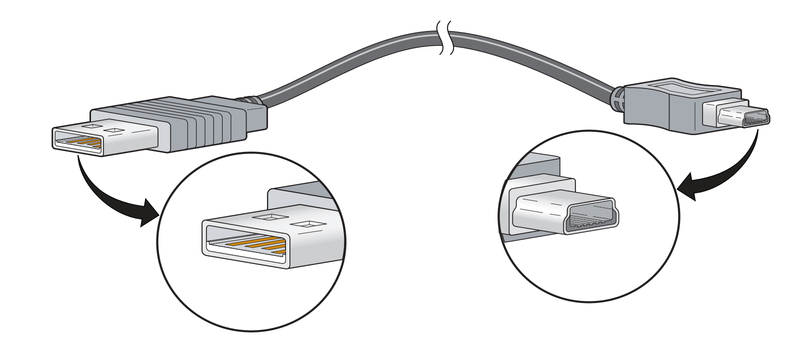
IMPORTANTE	La característica Auto-MDIX está habilitada de forma predeterminada. Para obtener información sobre la configuración de esta característica, consulte la guía de configuración del software del switch o la referencia de comandos del switch.

Puerto de consola

El switch tiene dos puertos de consola: un puerto USB mini tipo B de 5 pines en el panel frontal y un puerto de consola RJ45 en el panel trasero. No pueden estar activos los dos puertos de consola al mismo tiempo.

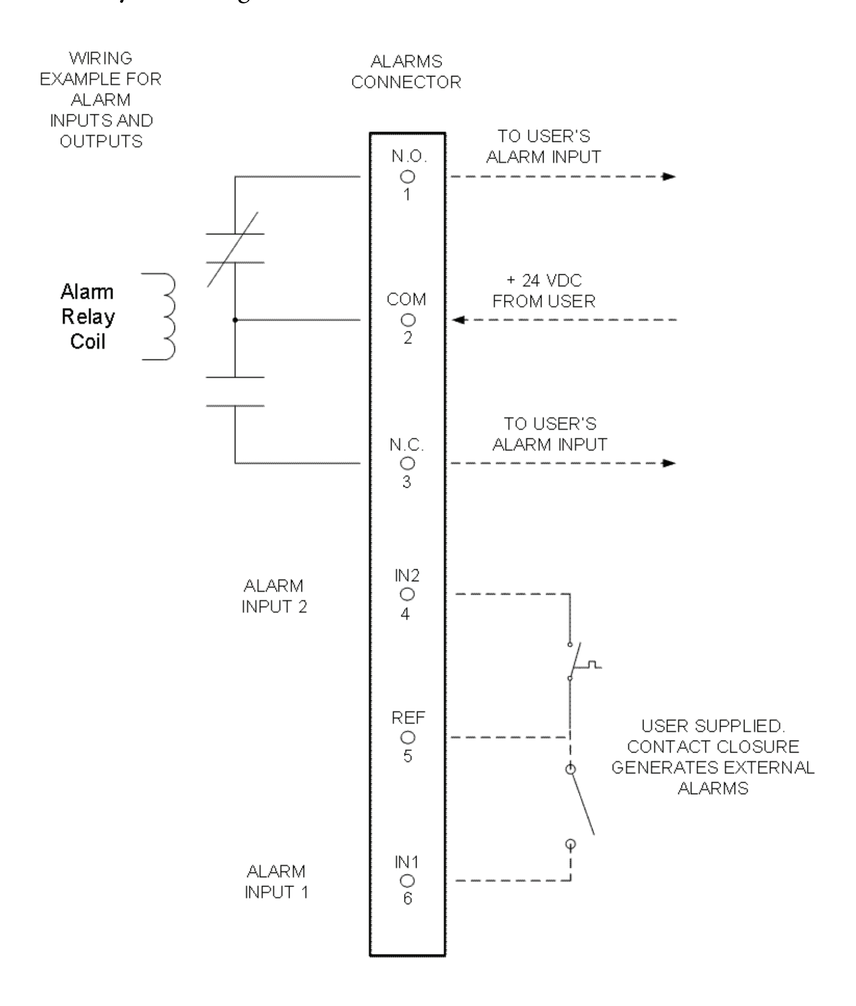


El puerto USB de consola utiliza un cable USB tipo A a USB mini tipo B de 5 pines. El cable USB tipo A a USB mini tipo B no se proporciona.



Puerto de alarma

Los puertos del conector de relé de alarma del panel frontal se describen en la ilustración y la tabla siguientes.



Etiqueta	Conexión
NO	Conexión de salida de alarma normalmente abierta (N.A.)
COM	Conexión común de salida de alarma
NC	Conexión de salida de alarma normalmente cerrada (N.C.)
IN2	Entrada de alarma 2
REF	Conexión de tierra de referencia de entrada de alarma
IN1	Entrada de alarma 1

Especificaciones de cables y adaptadores

Estas secciones describen los cables y los adaptadores utilizados con los switches.

Especificaciones de cables para módulos SFP

A continuación se enumeran las especificaciones de los cables para las conexiones de fibra óptica reforzadas del módulo SFP. Cada puerto debe cumplir con las especificaciones de longitud de onda en el otro extremo del cable y, para lograr una comunicación fiable, el cable no debe exceder la longitud máxima recomendada.

Tabla 46 - Especificaciones de cableado de puertos del módulo SFP de fibra óptica

Tipo de módulo SFP	N.° de cat.	Longitud de onda (nm)	Tipo de fibra	Tamaño del núcleo/ tamaño del revestimiento (micrones)	Ancho de banda modal (MHz/km)(1)	Distancia de cable
100BASE-FX	1783-SFP100FX	1310	MMF	50/125 62.5/125	500 500	2 km (6,562 pies) 2 km (6,562 pies)
100BASE-LX	1783-SFP100LX	1310	SMF	G.652[2]	—	10 km (32,810 pies)
1000BASE-SX	1783-SFP1GSX	850	MMF	62.5/125 62.5/125 50/125 50/125	160 200 400 500	220 m (722 pies) 275 m (902 pies)) 500 m (1640 pies) 550 m (1804 pies)
1000BASE-LX/LH	1783-SFP1GLX	1310	SMF	G.652[2]	—	10 km (32,810 pies)

(1) El ancho de banda modal solo se aplica a fibra multimodo.

Especificaciones de cables de puertos PoE

Para puertos PoE, utilice un cable de categoría 5 (Cat 5) de una longitud de 100 m (328 pies) como máximo.

Configuraciones de pines del adaptador

La tabla siguiente enumera las configuraciones de pines del puerto de consola, del cable adaptador RJ45 a DB-9 y del dispositivo de consola.

Tabla 47 - Configuraciones de pines del conector DB-9

Puerto de consola del switch (DTE)	Adaptador de terminales RJ45 a DB-9	Dispositivo de consola
Señal	**Pin del DB-9**	**Señal**
RTS	8	CTS
DTR	6	DSR
TxD	2	RxD
GND	5	GND
GND	5	GND
RxD	3	TxD
DSR	4	DTR
CTS	7	RTS

La tabla siguiente enumera las configuraciones de pines del puerto de consola, del adaptador DTE hembra RJ45 a DB-25 y del dispositivo de consola. El adaptador DTE hembra RJ45 a DB-25 no se suministra con el switch.

Tabla 48 - Configuraciones de pines del conector DB-25

Puerto de consola del switch (DTE)	Adaptador de terminales RJ45 a DB-25	Dispositivo de consola
Señal	**Pin del DB-25**	**Señal**
RTS	5	CTS
DTR	6	DSR
TxD	3	RxD
GND	7	GND
GND	7	GND
RxD	2	TxD
DSR	20	DTR
CTS	4	RTS

Notas:

Historial de cambios

Este apéndice resume las revisiones de este manual. Consulte este apéndice si necesita información para determinar los cambios que se han realizado a lo largo de las diferentes revisiones. Puede resultarle especialmente útil si tiene pensado actualizar el hardware o el software con base en la información añadida en las revisiones anteriores de este manual.

1783-UM004C-EN-P, Diciembre 2013

Cambio
Acceso a las notas de la versión del producto
Descripción de los switches con alimentación a través de Ethernet (PoE)
Dimensiones del switch PoE
Descripciones del puerto PoE
Calibre AWG del cable para conectar los tornillos de puesta a tierra externos
Cablee la fuente de alimentación PoE
Conecte el conector de alimentación PoE
Conecte puertos PoE
Express Setup y tarjeta SD
Numeración de los puertos en los switches con PoE
Descripciones de la característica PoE
Configure PoE a través de la interface web del administrador de dispositivos
Configuración de pines del conector del puerto PoE y especificaciones del cable

1783-UM004B-EN-P, Junio 2013

Cambio
La aplicación Studio 5000 Logix Designer™ es el nuevo nombre de marca asignado al software RSLogix 5000
Descripción de los switches 1783-BMS10CGN y 1783-BMS20CGN
Característica del software de traducción de direcciones de red (NAT)
Numeración de puertos de los switches 1783-BMS10CGN y 1783-BMS20CGN
Descripción general de NAT
Configure NAT a través de la interface web del administrador de dispositivos
Monitoree las estadísticas de NAT a través de la interface web del administrador de dispositivos
Configure NAT a través de la aplicación Logix Designer
Monitoree el diagnóstico de NAT a través de la aplicación Logix Designer

Índice

Servicio de asistencia técnica de Rockwell Automation

Rockwell Automation proporciona información técnica a través de Internet para ayudarle a utilizar sus productos. En http://www.rockwellautomation.com/support encontrará notas técnicas y de aplicación, ejemplos de códigos y vínculos a Service Packs de software. También puede visitar nuestro centro de asistencia técnica en https://rockwellautomation.custhelp.com/, donde encontrará actualizaciones de software, información técnica, chat y foros de asistencia técnica, respuestas a preguntas frecuentes, y podrá registrarse a fin de recibir actualizaciones de notificación de productos.

Además, ofrecemos varios programas de asistencia técnica para instalación, configuración y resolución de problemas. Para obtener más información, comuníquese con el distribuidor o representante de Rockwell Automation correspondiente a su localidad, o visite http://www.rockwellautomation.com/services/online-phone.

Asistencia para la instalación

Si se le presenta algún problema durante las primeras 24 horas posteriores a la instalación, revise la información incluida en este manual. También puede comunicarse con el servicio de asistencia técnica al cliente para obtener ayuda inicial con la puesta en marcha del producto.

Estados Unidos o Canadá	1.440.646.3434
Fuera de Estados Unidos o Canadá	Utilice Worldwide Locator en http://www.rockwellautomation.com/rockwellautomation/support/overview.page, o comuníquese con el representante de Rockwell Automation.

Devolución de productos nuevos

Rockwell Automation verifica todos sus productos antes de que salgan de la fábrica, para ayudar a garantizar su perfecto funcionamiento. No obstante, si su producto no funciona correctamente y necesita devolverlo, siga estos procedimientos.

En Estados Unidos	Comuníquese con el distribuidor. Deberá indicar al distribuidor un número de caso de asistencia técnica al cliente (llame al número de teléfono anterior para obtener uno) a fin de completar el proceso de devolución.
Fuera de Estados Unidos	Comuníquese con el representante local de Rockwell Automation para obtener información sobre el procedimiento de devolución.

Comentarios sobre la documentación

Sus comentarios nos ayudarán a atender mejor sus necesidades de documentación. Si tiene alguna sugerencia sobre cómo mejorar este documento, llene este formulario, publicación RA-DU002, disponible en http://www.rockwellautomation.com/literature/.

Rockwell Automation mantiene información medioambiental actualizada sobre sus productos en su sitio web en http://www.rockwellautomation.com/rockwellautomation/about-us/sustainability-ethics/product-environmental-compliance.page.

www.rockwellautomation.com

Oficinas corporativas de soluciones de potencia, control e información

Américas: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
Europa/Medio Oriente/África: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Bélgica, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
Asia-Pacífico: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Argentina: Rockwell Automation S.A., Alem 1050, 5º Piso, CP 1001AAS, Capital Federal, Buenos Aires, Tel.: (54) 11.5554.4000, Fax: (54) 11.5554.4040, www.rockwellautomation.com.ar
Chile: Rockwell Automation Chile S.A., Luis Thayer Ojeda 166, Piso 6, Providencia, Santiago, Tel.: (56) 2.290.0700, Fax: (56) 2.290.0707, www.rockwellautomation.cl
Colombia: Rockwell Automation S.A., Edf. North Point, Carrera 7 N° 156 – 78 Piso 18, PBX: (57) 1.649.96.00 Fax: (57)649.96.15, www.rockwellautomation.com.co
España: Rockwell Automation S.A., C/ Josep Plà, 101-105, 08019 Barcelona, Tel.: (34) 932.959.000, Fax: (34) 932.959.001, www.rockwellautomation.es
México: Rockwell Automation S.A. de C.V., Bosques de Cierulos N° 160, Col. Bosques de Las Lomas, C.P. 11700 México, D.F., Tel.: (52) 55.5246.2000, Fax: (52) 55.5251.1169, www.rockwellautomation.com.mx
Perú: Rockwell Automation S.A., Av Victor Andrés Belaunde N°147, Torre 12, Of. 102 – San Isidro Lima, Perú, Tel: (511) 441.59.00, Fax: (511) 222.29.87, www.rockwellautomation.com.pe
Puerto Rico: Rockwell Automation Inc., Calle 1, Metro Office # 6, Suite 304, Metro Office Park, Guaynabo, Puerto Rico 00968, Tel.: (1) 787.300.6200, Fax: (1) 787.706.3939, www.rockwellautomation.com.pr
Venezuela: Rockwell Automation S.A., Edf. Allen-Bradley, Av. González Rincones, Zona Industrial La Trinidad, Caracas 1080, Tel.: (58) 212.949.0611, Fax: (58) 212.943.3955, www.rockwellautomation.com.ve

Publicación 1783-UM004D-ES-P - Marzo 2014